(12)特許協力条約に基づいて公開された国際出願

(19) 世界知的所有権機関
国際事務局

(43) 国際公開日
2003年2月27日 (27.02.2003)

PCT

(10) 国際公開番号
WO 03/017273 A1

(51) 国際特許分類[7]: G11B 20/10, H04L 9/08, H04N 5/91

(21) 国際出願番号: PCT/JP02/07477

(22) 国際出願日: 2002年7月24日 (24.07.2002)

(25) 国際出願の言語: 日本語

(26) 国際公開の言語: 日本語

(30) 優先権データ:
特願2001-242041 2001年8月9日 (09.08.2001) JP

(71) 出願人 (米国を除く全ての指定国について): ソニー株式会社 (SONY CORPORATION) [JP/JP]; 〒141-0001 東京都 品川区 北品川６丁目７番３５号 Tokyo (JP).

(72) 発明者; および

(75) 発明者/出願人 (米国についてのみ): 浅野 智之 (ASANO,Tomoyuki) [JP/JP]; 〒141-0001 東京都 品川区 北品川６丁目７番３５号 ソニー株式会社内 Tokyo (JP). 中村 政信 (NAKAMURA,Masanobu) [JP/JP]; 〒141-0001 東京都 品川区 北品川６丁目７番３５号 ソニー株式会社内 Tokyo (JP).

(74) 代理人: 宮田 正昭, 外 (MIYATA,Masaaki et al.); 〒104-0041 東京都 中央区 新富一丁目１番７号 銀座ティーケイビル６階 澤田・宮田・山田特許事務所 Tokyo (JP).

(81) 指定国 (国内): CN, KR, US.

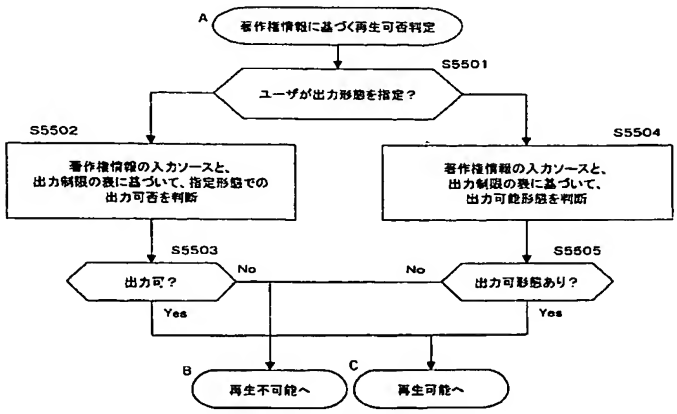
(84) 指定国 (広域): ヨーロッパ特許 (AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE, SK, TR).

添付公開書類:
— 国際調査報告書

２文字コード及び他の略語については、定期発行される各PCTガゼットの巻頭に掲載されている「コードと略語のガイダンスノート」を参照。

(54) Title: INFORMATION RECORING DEVICE, INFORMATION REPRODUCING DEVICE, INFORMATION RECORING METHOD, INFORMATION REPRODUCING METHOD, AND COMPUTER PROGRAM

(54) 発明の名称: 情報記録装置、情報再生装置、および情報記録方法、情報再生方法、並びにコンピュータ・プログラム



A JUDGE FROM COPYRIGHT INFORMATION WHETHER REPRODUCTION IS ALLOWED OR NOT
S5501 OUTPUT MODE SPECIFIED BY USER?
S5502...JUDGE FROM INPUT SOURCE OF COPYRIGHT INFORMATION AND LIST OF OUTPUT RESTRICTION WHETHER OUTPUT IN SPECIFIED MODE IS ALLOWED OR NOT
S5503...OUTPUT ALLOWED?
S5504...IDENTIFY OUTPUT-ALLOWED MODE ON THE BASIS OF INPUT SOURCE OF COPYRIGHT INFORMATION AND LIST OF OUTPUT RESTRICTION
S5505...ANY OUTPUT-ALLOWED MODE?
B...REPRODUCTION IS MADE ALLOWED
C...REPRODUCTION IS MADE NOT ALLOWED

(57) Abstract: A recording/reproducing device that carries out a control for adaptation of content recording/reproduction to copyright accurately and efficiently. Input source information on recorded contents is stored as adaptation copyright information on stored contents stored on a record medium. To reproduce a content, the input source information is acquired,

[続葉有]

WO 03/017273 A1

and it is judged from the acquired input source information whether reproduction/outputting is allowed or not. Correct content reproduction restriction corresponding to output restriction depending on the input source is realized. The key needed to generate a MAC for the copyright information is transmitted together with the enabling key block (EKB) conforming to the key distribution system of a tree structure. Therefore MAC validation of only authorized license device is possible. Consequently, a content having a structure allowing authorized use is realized.

(57) 要約:

コンテンツ記録再生における正確かつ効率的な著作権対応制御を可能とした記録再生装置を提供する。記録媒体の格納コンテンツの対応著作権情報として、記録コンテンツの入力ソース情報を格納した。コンテンツ再生に際して、入力ソース情報を取得して、取得情報に基づいて、再生、出力の可否を判定する。入力ソースに応じた様々な出力制限に応じた正確なコンテンツ再生制限が可能となる。また、著作権情報に対するＭＡＣの生成に必要なキーをツリー（木）構造の鍵配布構成に従った有効化キーブロック（ＥＫＢ）とともに送信する構成としたので、正当なライセンス・デバイスにおいてのみＭＡＣ検証が可能となり、コンテンツの正当な利用構成が実現される。

明 細 書

情報記録装置、情報再生装置、および情報記録方法、情報再生方法、並びにコンピュータ・プログラム

技術分野

本発明は、情報記録装置、情報再生装置、および情報記録方法、情報再生方法、並びにコンピュータ・プログラムに関し、さらに詳細には、著作権保護等を目的とした利用制限の付加されたコンテンツの記録媒体に対する格納処理、および記録媒体からの再生処理の改良を図った情報記録装置、情報再生装置、および情報記録方法、情報再生方法、並びにコンピュータ・プログラムに関する。

背景技術

デジタル信号処理技術の進歩、発展に伴い、近年においては、情報をデジタル的に記録する記録装置や記録媒体が普及しつつある。このようなデジタル記録装置および記録媒体によれば、例えば画像や音声を劣化させることなく記録、再生を繰り返すことができる。このようにデジタルデータは画質や音質を維持したまま何度もコピーを繰り返し実行することができるため、コピーが違法に行われた記録媒体が市場に流通することになると、音楽、映画等各種コンテンツの著作権者、あるいは正当な販売権者等の利益が害されることになる。昨今では、このようなデジタルデータの不正なコピーを防ぐため、デジタル記録装置および記録媒体に違法なコピーを防止するための様々な処理構成が実現または提案されている。

違法なコピーを防止するため、コンテンツに対応付けたコピー制御情報が用いられる。代表的なコピー制御情報としては、ＳＣＭＳ：Serial Copy Management SystemやＣＧＭＳ：Copy Generation Management Systemがある。これらのコピー制御情報の内容は、その情報が付加されたデータは制限なくコピーが許可されていることを示すコピーフリー（Copy Free)、1 世代のみのコピーを許可する 1 世代コピー許可（One Generation Copy Allowed)、コピーを認めないコピー禁止（Copy Prohibited）などの情報である。

ＣＧＭＳ方式は、アナログ映像信号（ＣＧＭＳ－Ａと呼ばれる）であれば、その輝度信号の垂直ブランキング期間内の特定の１水平区間、例えばＮＴＳＣ信号の場合には、第２０水平区間の有効映像部分に重畳する２０ビットの付加情報のうちの２ビットを複製制御用の情報として重畳し、また、デジタル映像信号（ＣＧＭＳ－Ｄと呼ばれる）であれば、デジタル映像データに挿入付加する付加情報として、複製制御用の２ビットの情報を含めて伝送する方式である。

このＣＧＭＳ方式の場合の２ビットの情報（以下、ＣＧＭＳ情報という）の意味内容は、［００］……複製可能［１０］……１回複製可能（１世代だけ複製可能）［１１］……複製禁止（絶対複製禁止）

である。

映像情報に付加されたＣＧＭＳ情報が［１０］であった場合に、ＣＧＭＳ対応の記録装置では、その映像情報の複製記録が可能であると判断して記録を実行するが、記録された映像信号には［１１］に書き換えられたＣＧＭＳ情報が付加される。そして、記録しようとする映像情報に付加されたＣＧＭＳ情報が［１１］の場合には、ＣＧＭＳ対応の記録装置では、その画像信号の複製記録は禁止であるとして記録の実行が禁止される。デジタル映像データのインターフェースとして、ＩＥＥＥ１３９４インターフェースがあるが、このインターフェースにおいては、ＣＧＭＳ情報を用いて著作権保護を行う方法が提案されている。

また、例えば、ＭＤ（ミニディスク）（ＭＤは商標）装置において、違法なコピーを防止する方法として、ＳＣＭＳ(Serial Copy Management System)が採用されている。ＳＣＭＳは、データ再生側において、オーディオデータとともにＳＣＭＳ信号をデジタルインタフェース（ＤＩＦ）から出力し、データ記録側において、再生側からのＳＣＭＳ信号に基づいて、再生側からのオーディオデータの記録を制御することにより違法なコピーを防止するシステムである。

具体的にはＳＣＭＳ信号は、オーディオデータが、何度でもコピーが許容されるコピーフリー（copy free）のデータであるか、１度だけコピーが許されている（copy once allowed）データであるか、またはコピーが禁止されている（copy prohibited）データであるかを表す信号である。データ記録側において、ＤＩＦからオーディオデータを受信すると、そのオーディオデータとともに送信される

ＳＣＭＳ信号を検出する。そして、ＳＣＭＳ信号が、コピーフリー（copy free）となっている場合には、オーディオデータをＳＣＭＳ信号とともにミニディスクに記録する。また、ＳＣＭＳ信号が、コピーを１度のみ許可（copy once allowed）となっている場合には、ＳＣＭＳ信号をコピー禁止（copy prohibited）に変更して、オーディオデータとともに、ミニディスクに記録する。さらに、ＳＣＭＳ信号が、コピー禁止（copy prohibited）となっている場合には、オーディオデータの記録を行わない。このようなＳＣＭＳを使用した制御を行なうことで、ミニディスク装置では、ＳＣＭＳによって、著作権を有するオーディオデータが、違法にコピーされるのを防止するようになっている。

上述のコピー制御情報を具体的に適用した構成としては、本特許出願人であるソニー株式会社を含む企業５社の共同体の提案する５Ｃ－ＤＴＣＰ（Digital Transmission Content Protection）に従ったコピー制御情報（ＣＣＩ：Copy Control Information)がある。これは、ＩＥＥＥ１３９４インタフェースからのコンテンツ入力の場合や、衛星・地上波のデジタルテレビ放送などにおけるコンテンツに対するコピー制御情報（ＣＣＩ：Copy Control Information)の送信方法を規定し、またコンテンツを記録、再生する記録再生装置におけるコピー制御処理を規定している。

さらに、上述の手法以外に、電子透かし（ウォーターマーク（ＷＭ））を用いたコピー制御情報の付加構成がある。電子透かし（ウォーターマーク（ＷＭ））は、通常のコンテンツ（画像データまたは音声データ）の再生状態では視覚あるいは知覚困難なデータをコンテンツに重畳し、例えばコンテンツの記録、再生等の際に電子透かしを検出して、制御を行なうものである。コンテンツがアナログデータであっても電子透かしの埋め込み、検出が可能であり用途は広い。しかし、電子透かしの検出、埋め込み処理専用の構成が必要となる。

発明の開示

上述したように、コンテンツの著作権保護を目的としたコピー制御情報のコンテンツに対する付加手法は多様であり、コンテンツを格納し、再生する記録再生装置としても、上述した様々なコピー制御情報の処理が可能な対応機器、不可能

な非対応機器等、様々な機器が存在する。

このように多様な機器が存在する現状では、機器間のコンテンツ入出力、コピー処理が実行された場合、コピー制御情報の正確な取り扱いが困難になる場合がある。例えば上述した５Ｃ－ＤＴＣＰ（Digital Transmission Content Protection）システムで提唱するコピー制御情報（ＣＣＩ：Copy Control Information)と、電子透かし（ウォーターマーク（ＷＭ））を用いたコピー制御情報との双方が付加されたコンテンツについての処理を実行する場合、コンテンツ処理装置が電子透かし（ウォーターマーク（ＷＭ））の検出が実行できない機器である場合、電子透かし（ウォーターマーク（ＷＭ））の検出は可能であるが、埋め込み処理が実行できない機器である場合、検出、埋め込みの双方が可能な機器である場合などにおいて、ＣＣＩおよび電子透かし各コピー制御情報の読み取り、書き換え処理が機器に応じて異なる態様で実行され、正確な更新処理が実行されないなどの事態が発生する。

例えば、電子透かし（ウォーターマーク（ＷＭ））の検出値に応じて、ＣＣＩの書き換えを行なう機器があり、また、電子透かし（ウォーターマーク（ＷＭ））の検出値を取得せずにＣＣＩの書き換えのみを行なったり、あるいは電子透かし(ウォーターマーク（ＷＭ））と、ＣＣＩとの双方を書き換えるなど、その機器の処理可能な態様に応じて様々な処理が実行される。この結果、ＣＣＩとＷＭの不整合の問題等が発生し、正しいコピー制御が実行不可能になる場合がある。

さらに、記録コンテンツの入力ソースによっては、記録媒体に記録したコンテンツの出力態様を制限する要求を伴ってコンテンツを提供するソースがある。このような場合、入力ソースの情報を破棄してしまうと、予め入力ソースに応じて規定された再生制限が正確に実行されず、コンテンツ再生、コンテンツコピーが無秩序に実行される可能性がある。

本発明は、上述の問題点に鑑みてなされたものであり、様々なコンテンツ入力ソースがあり、また、様々なコピー制御情報取り扱い機器が混在する現状において、入力ソースに応じ、またコンテンツに付与されたコピー制御情報に従った正確なコンテンツ制御を実行可能とした情報記録装置、情報再生装置、および情報記録方法、情報再生方法、並びにコンピュータ・プログラムを提供することを目

的とする。

本発明の第１の側面は、

コンテンツの記録媒体に対する記録処理を実行する情報記録装置であり、

記録媒体に対する記録対象コンテンツに関する入力ソース情報を含む著作権情報を生成し、前記記録対象コンテンツを格納する記録媒体に格納する処理を実行する構成を有することを特徴とする情報記録装置にある。

さらに、本発明の情報記録装置の一実施態様において、前記情報記録装置は、前記入力ソース情報を含む著作権情報に対応する改竄チェック用データを生成し、記録媒体に対して格納する著作権情報とともに格納する構成を有することを特徴とする。

さらに、本発明の情報記録装置の一実施態様において、前記入力ソース情報は、ＩＥＥＥ１３９４インタフェースを介するコピー制御情報を持つコンテンツ入力であるか否かを示す情報を含むことを特徴とする。

さらに、本発明の情報記録装置の一実施態様において、前記入力ソース情報は、デジタルデータ入力であるかアナログデータ入力であるかを示す情報を含むことを特徴とする。

さらに、本発明の情報記録装置の一実施態様において、前記入力ソース情報は、入力コンテンツに対して設定されたコピー制御情報態様を含み、デジタルデータとしてのＴＳパケットに付加されたコピー制御情報を有するか、または電子透かしとして付加されたコピー制御情報を有するかを示す情報を含むことを特徴とする。

さらに、本発明の情報記録装置の一実施態様において、前記情報記録装置は、複数の異なる情報記録装置をリーフとした階層ツリー構造を構成する各ノードに固有のノードキーと各情報記録装置固有のリーフキーとを格納し、ノードキーを下位階層のノードキーまたはリーフキーの少なくともいずれかを含むキーにより暗号化した有効化キーブロック（ＥＫＢ）の復号処理を実行し、該復号処理によって取得可能な鍵を適用して、前記入力ソース情報を含む著作権情報に対応する改竄チェック用データを生成し、記録媒体に対して格納する著作権情報とともに格納する構成を有することを特徴とする。

さらに、本発明の情報記録装置の一実施態様において、前記情報記録装置は、複数の異なる情報記録装置をリーフとした階層ツリー構造を構成する各ノードに固有のノードキーと各情報記録装置固有のリーフキーとを格納し、ノードキーを下位階層のノードキーまたはリーフキーの少なくともいずれかを含むキーにより暗号化した有効化キーブロック（ＥＫＢ）の復号処理を実行し、該復号処理によって取得可能な鍵を適用して、前記入力ソース情報を含む著作権情報に対応する改竄チェック用データを生成し、記録媒体に対して格納する著作権情報とともに格納する構成を有するとともに、前記有効化キーブロック（ＥＫＢ）の復号処理を実行し、該復号処理によって取得可能な鍵を適用して取得される鍵に基づいて、記録対象コンテンツの暗号化処理を実行して記録媒体に対して格納する処理を実行する構成を有することを特徴とする。

さらに、本発明の第２の側面は、

コンテンツの記録媒体からの再生処理を実行する情報再生装置であり、

記録媒体からの再生対象コンテンツに関する入力ソース情報を含む著作権情報を、前記再生対象コンテンツ格納記録媒体から読み出して、前記再生対象コンテンツの入力ソース情報に対応した出力制限に基づく再生制御を行なう構成を有することを特徴とする情報再生装置にある。

さらに、本発明の情報再生装置の一実施態様において、前記情報再生装置は、前記入力ソース情報を含む著作権情報に対応する改竄チェック用データを、前記再生対象コンテンツ格納記録媒体から読み出した著作権情報に基づいて生成し、該生成データと、前記記録媒体に格納済みの改竄チェック値との照合により、著作権情報の改竄検証を実行し、改竄無しの結果取得を条件として、コンテンツ再生処理を実行する構成を有することを特徴とする。

さらに、本発明の情報再生装置の一実施態様において、前記入力ソース情報は、ＩＥＥＥ１３９４インタフェースを介するコピー制御情報を持つコンテンツ入力であるか否かを示す情報を含むことを特徴とする。

さらに、本発明の情報再生装置の一実施態様において、前記入力ソース情報は、デジタルデータ入力であるかアナログデータ入力であるかを示す情報を含むことを特徴とする。

さらに、本発明の情報再生装置の一実施態様において、前記入力ソース情報は、入力コンテンツに対して設定されたコピー制御情報態様を含み、デジタルデータとしてのＴＳパケットに付加されたコピー制御情報を有するか、または電子透かしとして付加されたコピー制御情報を有するかを示す情報を含むことを特徴とする。

さらに、本発明の情報再生装置の一実施態様において、前記情報再生装置は、複数の異なる情報再生装置をリーフとした階層ツリー構造を構成する各ノードに固有のノードキーと各情報再生装置固有のリーフキーとを格納し、ノードキーを下位階層のノードキーまたはリーフキーの少なくともいずれかを含むキーにより暗号化した有効化キーブロック（ＥＫＢ）の復号処理を実行し、該復号処理によって取得可能な鍵を適用して、前記入力ソース情報を含む著作権情報に対応する改竄チェック用データを生成し、著作権情報の改竄検証を実行する構成を有することを特徴とする。

さらに、本発明の情報再生装置の一実施態様において、前記情報再生装置は、複数の異なる情報再生装置をリーフとした階層ツリー構造を構成する各ノードに固有のノードキーと各情報再生装置固有のリーフキーとを格納し、ノードキーを下位階層のノードキーまたはリーフキーの少なくともいずれかを含むキーにより暗号化した有効化キーブロック（ＥＫＢ）の復号処理を実行し、該復号処理によって取得可能な鍵を適用して、前記入力ソース情報を含む著作権情報に対応する改竄チェック用データを生成し、著作権情報の改竄検証を実行する構成を有するとともに、前記有効化キーブロック（ＥＫＢ）の復号処理を実行し、該復号処理によって取得可能な鍵を適用して取得される鍵に基づいて、再生対象コンテンツの復号処理を実行して記録媒体からのコンテンツ再生処理を実行する構成を有することを特徴とする。

さらに、本発明の第３の側面は、

コンテンツの記録媒体に対する記録処理を実行する情報記録方法であり、

記録媒体に対する記録対象コンテンツに関する入力ソース情報を含む著作権情報を生成し、前記記録対象コンテンツを格納する記録媒体に格納する処理を実行することを特徴とする情報記録方法にある。

さらに、本発明の情報記録方法の一実施態様において、前記情報記録方法は、さらに、前記入力ソース情報を含む著作権情報に対応する改竄チェック用データを生成し、記録媒体に対して格納する著作権情報とともに格納することを特徴とする。

さらに、本発明の情報記録方法の一実施態様において、前記入力ソース情報は、ＩＥＥＥ１３９４インタフェースを介するコピー制御情報を持つコンテンツ入力であるか否かを示す情報を含むことを特徴とする。

さらに、本発明の情報記録方法の一実施態様において、前記入力ソース情報は、デジタルデータ入力であるかアナログデータ入力であるかを示す情報を含むことを特徴とする。

さらに、本発明の情報記録方法の一実施態様において、前記入力ソース情報は、入力コンテンツに対して設定されたコピー制御情報態様を含み、デジタルデータとしてのＴＳパケットに付加されたコピー制御情報を有するか、または電子透かしとして付加されたコピー制御情報を有するかを示す情報を含むことを特徴とする。

さらに、本発明の情報記録方法の一実施態様において、前記情報記録方法を実行する情報記録装置は、複数の異なる情報記録装置をリーフとした階層ツリー構造を構成する各ノードに固有のノードキーと各情報記録装置固有のリーフキーとを格納し、前記情報記録方法において、ノードキーを下位階層のノードキーまたはリーフキーの少なくともいずれかを含むキーにより暗号化した有効化キーブロック（ＥＫＢ）の復号処理を実行し、該復号処理によって取得可能な鍵を適用して、前記入力ソース情報を含む著作権情報に対応する改竄チェック用データを生成し、記録媒体に対して格納する著作権情報とともに格納する処理を実行することを特徴とする。

さらに、本発明の情報記録方法の一実施態様において、前記情報記録方法を実行する情報記録装置は、複数の異なる情報記録装置をリーフとした階層ツリー構造を構成する各ノードに固有のノードキーと各情報記録装置固有のリーフキーとを格納し、前記情報記録方法において、ノードキーを下位階層のノードキーまたはリーフキーの少なくともいずれかを含むキーにより暗号化した有効化キーブロ

ック（ＥＫＢ）の復号処理を実行し、該復号処理によって取得可能な鍵を適用して、前記入力ソース情報を含む著作権情報に対応する改竄チェック用データを生成し、記録媒体に対して格納する著作権情報とともに格納するとともに、前記有効化キーブロック（ＥＫＢ）の復号処理を実行し、該復号処理によって取得可能な鍵を適用して取得される鍵に基づいて、記録対象コンテンツの暗号化処理を実行して記録媒体に対して格納する処理を実行することを特徴とする。

さらに、本発明の第４の側面は、

コンテンツの記録媒体からの再生処理を実行する情報再生方法であり、

記録媒体からの再生対象コンテンツに関する入力ソース情報を含む著作権情報を、前記再生対象コンテンツ格納記録媒体から読み出して、前記再生対象コンテンツの入力ソース情報に対応した出力制限に基づく再生制御を行なうことを特徴とする情報再生方法にある。

さらに、本発明の情報再生方法の一実施態様において、前記情報再生方法は、さらに、前記入力ソース情報を含む著作権情報に対応する改竄チェック用データを、前記再生対象コンテンツ格納記録媒体から読み出した著作権情報に基づいて生成し、該生成データと、前記記録媒体に格納済みの改竄チェック値との照合により、著作権情報の改竄検証を実行し、改竄無しの結果取得を条件として、コンテンツ再生処理を実行することを特徴とする。

さらに、本発明の情報再生方法の一実施態様において、前記入力ソース情報は、ＩＥＥＥ１３９４インタフェースを介するコピー制御情報を持つコンテンツ入力であるか否かを示す情報を含むことを特徴とする。

さらに、本発明の情報再生方法の一実施態様において、前記入力ソース情報は、デジタルデータ入力であるかアナログデータ入力であるかを示す情報を含むことを特徴とする。

さらに、本発明の情報再生方法の一実施態様において、前記入力ソース情報は、入力コンテンツに対して設定されたコピー制御情報態様を含み、デジタルデータとしてのＴＳパケットに付加されたコピー制御情報を有するか、または電子透かしとして付加されたコピー制御情報を有するかを示す情報を含むことを特徴とする。

さらに、本発明の情報再生方法の一実施態様において、前記情報再生方法を実行する情報再生装置は、複数の異なる情報再生装置をリーフとした階層ツリー構造を構成する各ノードに固有のノードキーと各情報再生装置固有のリーフキーとを格納し、前記情報再生方法において、ノードキーを下位階層のノードキーまたはリーフキーの少なくともいずれかを含むキーにより暗号化した有効化キーブロック（ＥＫＢ）の復号処理を実行し、該復号処理によって取得可能な鍵を適用して、前記入力ソース情報を含む著作権情報に対応する改竄チェック用データを生成し、著作権情報の改竄検証を実行することを特徴とする。

さらに、本発明の情報再生方法の一実施態様において、前記情報再生方法を実行する情報再生装置は、複数の異なる情報再生装置をリーフとした階層ツリー構造を構成する各ノードに固有のノードキーと各情報再生装置固有のリーフキーとを格納し、前記情報再生方法において、ノードキーを下位階層のノードキーまたはリーフキーの少なくともいずれかを含むキーにより暗号化した有効化キーブロック（ＥＫＢ）の復号処理を実行し、該復号処理によって取得可能な鍵を適用して、前記入力ソース情報を含む著作権情報に対応する改竄チェック用データを生成し、著作権情報の改竄検証を実行するとともに、前記有効化キーブロック（ＥＫＢ）の復号処理を実行し、該復号処理によって取得可能な鍵を適用して取得される鍵に基づいて、再生対象コンテンツの復号処理を実行して記録媒体からのコンテンツ再生処理を実行することを特徴とする。

さらに、本発明の第５の側面は、

コンテンツの記録媒体に対する記録処理をコンピュータ・システム上で実行せしめるコンピュータ・プログラムであって、

記録媒体に対する記録対象コンテンツに関する入力ソース情報を含む著作権情報を生成するステップと、

前記記録対象コンテンツを格納する記録媒体に格納する処理ステップと、

を具備することを特徴とするコンピュータ・プログラムにある。

さらに、本発明の第６の側面は、

コンテンツの記録媒体からの再生処理をコンピュータ・システム上で実行せしめるコンピュータ・プログラムであって、

記録媒体からの再生対象コンテンツに関する入力ソース情報を含む著作権情報を、前記再生対象コンテンツ格納記録媒体から読み出すステップと、

前記再生対象コンテンツの入力ソース情報に対応した出力制限に基づく再生制御を行なうステップと、

を具備することを特徴とするコンピュータ・プログラムにある。

なお、本発明のコンピュータ・プログラムは、例えば、様々なプログラム・コードを実行可能なコンピュータ・システムに対して、コンピュータ可読形式で提供する記憶媒体、通信媒体、例えば、ＣＤやＦＤ、ＭＯなどの記録媒体、あるいは、ネットワークなどの通信媒体によって提供可能なコンピュータ・プログラムである。このようなプログラムをコンピュータ可読な形式で提供することにより、コンピュータ・システム上でプログラムに応じた処理が実現される。

本発明のさらに他の目的、特徴や利点は、後述する本発明の実施例や添付する図面に基づくより詳細な説明によって明らかになるであろう。なお、本明細書においてシステムとは、複数の装置の論理的集合構成であり、各構成の装置が同一筐体内にあるものには限らない。

図面の簡単な説明

図１は、本発明の記録再生装置の構成例（その１）を示すブロック図である。

図２は、本発明の記録再生装置の構成例（その２）を示すブロック図である。

図３は、本発明の記録再生装置のデータ記録処理フローを示す図である。

図４は、本発明の記録再生装置のデータ再生処理フローを示す図である。

図５は、本発明の記録再生装置において処理されるデータフォーマットを説明する図である。

図６は、本発明の記録再生装置におけるトランスポート・ストリーム（ＴＳ）処理手段の構成を示すブロック図である。

図７は、本発明の記録再生装置において処理されるトランスポート・ストリームの構成を説明する図である。

図８は、本発明の記録再生装置におけるトランスポート・ストリーム（ＴＳ）処理手段の構成を示すブロック図である。

図９は、本発明の記録再生装置におけるトランスポート・ストリーム（ＴＳ）処理手段の構成を示すブロック図である。

図１０は、本発明の記録再生装置において処理されるブロックデータの付加情報としてのブロック・データの構成例を示す図である。

図１１は、入力ソースの出力制限の規則例を示す図である。

図１２は、本発明の記録再生装置において処理される伝送１３９４パケットにおけるＥＭＩ格納位置（５ＣＤＴＣＰ規格）を示す図である。

図１３は、本発明の記録再生装置における著作権情報のデータとしてのコピー制御情報変化点情報の構成例を示す図である。

図１４は、本発明の記録再生装置に対するマスターキー、メディアキー等の鍵の暗号化処理について説明するツリー構成図である。

図１５は、本発明の記録再生装置に対するマスターキー、メディアキー等の鍵の配布に使用される有効化キーブロック（ＥＫＢ）の例を示す図である。

図１６は、本発明の記録再生装置におけるマスターキーの有効化キーブロック（ＥＫＢ）を使用した配布例と復号処理例を示す図である。

図１７は、本発明の記録再生装置におけるマスターキーの有効化キーブロック（ＥＫＢ）を使用した復号処理フローを示す図である。

図１８は、本発明の記録再生装置におけるコンテンツ記録処理におけるマスターキーの世代比較処理フローを示す図である。

図１９は、本発明の記録再生装置において、データ記録処理時の暗号化処理を説明するブロック図（その１）である。

図２０は、本発明の記録再生装置において、データ記録処理時の暗号化処理を説明するブロック図（その２）である。

図２１は、本発明の記録再生装置におけるディスク固有キーの生成例を説明する図である。

図２２は、本発明の記録再生装置におけるコンテンツ記録をデータ解析記録方式(Cognizant Mode)によって実行するか、データ非解析記録方式(Non-Cognizant Mode)で実行するかを決定するプロセスを説明するフロー図である。

図２３は、本発明の記録再生装置において、データ記録時のタイトル固有キー

の生成処理例を示す図である。

図２４は、本発明の記録再生装置におけるブロック・キーの生成方法を説明する図である。

図２５は、本発明の記録再生装置における著作権情報格納処理例(例１)を示すフロー図である。

図２６は、本発明の記録再生装置における著作権情報格納処理例(例２)を示すフロー図である。

図２７は、本発明の記録再生装置における著作権情報格納処理例(例３)を示すフロー図である。

図２８は、本発明の記録再生装置における著作権情報ＭＡＣ算出処理例を示す図である。

図２９は、本発明の記録再生装置において、データ記録処理を説明するフローチャートである。

図３０は、本発明の記録再生装置におけるタイトル固有キーの生成処理フローを示す図である。

図３１は、本発明の記録再生装置において、データ再生処理時のコンテンツデータ復号処理を説明するブロック図である。

図３２は、本発明の記録再生装置において、データ再生処理を説明するフローチャートである。

図３３は、本発明の記録再生装置において、データ再生処理における再生可能制判定処理の詳細を示すフローチャートである。

図３４は、本発明の記録再生装置において、データ再生処理における著作権情報に基づく再生可能制判定処理（例１）を示すフローチャートである。

図３５は、本発明の記録再生装置において、データ再生処理における著作権情報に基づく再生可能制判定処理（例２）を示すフローチャートである。

図３６は、本発明の記録再生装置において、データ再生処理における著作権情報に基づく再生可能制判定処理（例３）を示すフローチャートである。

図３７は、本発明の記録再生装置において、データ再生時のタイトル固有キーの生成処理フローを示す図である。

図３８は、本発明の記録再生装置において、データ再生処理における著作権情報に基づく再生処理（例１）を示すフローチャートである。

図３９は、本発明の記録再生装置において、データ再生処理における著作権情報に基づく再生処理（例２）を示すフローチャートである。

図４０は、本発明の記録再生装置におけるメディアキーの有効化キーブロック（ＥＫＢ）を使用した配布例と復号処理例を示す図である。

図４１は、本発明の記録再生装置におけるメディアキーの有効化キーブロック（ＥＫＢ）を使用した復号処理フローを示す図である。

図４２は、本発明の記録再生装置におけるメディアキーを使用したコンテンツ記録処理フローを示す図である。

図４３は、本発明の記録再生装置において、メディアキーを使用したデータ記録処理時の暗号化処理を説明するブロック図（その１）である。

図４４は、本発明の記録再生装置において、メディアキーを使用したデータ記録処理時の暗号化処理を説明するブロック図（その２）である。

図４５は、本発明の記録再生装置において、メディアキーを使用したデータ記録処理を説明するフローチャートである。

図４６は、本発明の記録再生装置において、メディアキーを使用したデータ再生処理時の暗号処理を説明するブロック図である。

図４７は、本発明の記録再生装置において、メディアキーを使用したデータ再生処理を説明するフローチャートである。

図４８は、本発明の記録再生装置において、メディアキーを使用したデータ再生処理における再生可能性判定処理の詳細を示すフローチャートである。

図４９は、情報記録再生装置の処理手段構成を示したブロック図である。

発明を実施するための最良の形態

以下、本発明の構成について図面を参照して詳細に説明する。なお、説明手順は、以下の項目に従って行なう。

１．記録再生装置の構成

２．記録、再生処理

3．トランスポートストリーム（ＴＳ）処理

4．電子透かし（WM）処理

5．著作権情報

6．キー配信構成としてのツリー（木）構造について

7．マスターキーを用いた暗号処理によるコンテンツの記録再生

8．メディアキーを用いた暗号処理によるコンテンツの記録再生

9．記録再生装置ハードウェア構成

［１．記録再生装置の構成］

図１は、本発明の情報処理装置としての記録再生装置１００の一実施例構成を示すブロック図である。記録再生装置１００は、例えば、データ記録再生可能なＲＡＭディスクを装着し、ＲＡＭディスクに対するデータの読書きを実行するＤＶＲシステム、あるいはデータ記録再生可能なハードディスクを装着し、ハードディスクに対するデータの読書きを実行するＨＤＲシステムなどであり、ＤＶＤ、ＣＤ等の光ディスク、光磁気ディスク、ＨＤ等の磁気ディスク、磁気テープ、あるいはＲＡＭ等の半導体メモリ等のデジタルデータの記憶可能な媒体に対するデータの記録再生を実行する装置である。

記録再生装置１００は、入出力Ｉ／Ｆ(Interface)として、ＵＳＢ対応の入出力Ｉ／Ｆ(Interface)１２１、ＩＥＥＥ１３９４対応の入出力Ｉ／Ｆ(Interface)１２２、ＭＰＥＧ(Moving Picture Experts Group)コーデック１３０、Ａ／Ｄ，Ｄ／Ａコンバータ１４１を備えたアナログデータ対応の入出力Ｉ／Ｆ(Interface)１４０、暗号処理手段１５０、ＲＯＭ(Read Only Memory)１６０、ＣＰＵ(Central Processing Unit)１７０、メモリ１８０、記録媒体１９５のドライブ１９０、トランスポート・ストリーム処理手段（ＴＳ処理手段）３００、電子透かし（ウォーターマーク（WM)）検出、埋め込み手段１８５、さらに、地上波ＲＦ信号を受信する地上波チューナ，コンバータ５０１、衛星波ＲＦ信号を受信する衛星波チューナ，コンバータ５０２を有し、これらはバス１１０によって相互に接続されている。

入出力Ｉ／Ｆ１２１，１２２は、外部からそれぞれＵＳＢ，ＩＥＥＥ１３９４バス介して供給される画像、音声、プログラム等の各種コンテンツを構成するデ

ジタル信号を受信し、バス１１０上に出力するとともに、バス１１０上のデジタル信号を受信し、外部に出力する。ＭＰＥＧコーデック１３０は、バス１１０を介して供給されるＭＰＥＧ符号化されたデータを、ＭＰＥＧデコードし、入出力Ｉ／Ｆ１４０に出力するとともに、入出力Ｉ／Ｆ１４０から供給されるデジタル信号をＭＰＥＧエンコードしてバス１１０上に出力する。入出力Ｉ／Ｆ１４０は、Ａ／Ｄ，Ｄ／Ａコンバータ１４１を内蔵している。入出力Ｉ／Ｆ１４０は、外部から供給されるコンテンツとしてのアナログ信号を受信し、Ａ／Ｄ，Ｄ／Ａコンバータ１４１でＡ／Ｄ(Analog Digital)変換することで、デジタル信号として、ＭＰＥＧコーデック１３０に出力するとともに、ＭＰＥＧコーデック１３０からのデジタル信号を、Ａ／Ｄ，Ｄ／Ａコンバータ１４１でＤ／Ａ(Digital Analog)変換することで、アナログ信号として、外部に出力する。

暗号処理手段１５０は、例えば、１チップのＬＳＩ(Large Scale Integrated Circuit)で構成され、バス１１０を介して供給されるコンテンツとしてのデジタル信号を暗号化し、または復号し、バス１１０上に出力する構成を持つ。なお、暗号処理手段１５０は１チップＬＳＩに限らず、各種のソフトウェアまたはハードウェアを組み合わせた構成によって実現することも可能である。ソフトウェア構成による処理手段としての構成については後段で説明する。

ＲＯＭ１６０は、例えば、記録再生装置ごとに固有の、あるいは複数の記録再生装置のグループごとに固有のデバイスキーであるリーフキーと、複数の記録再生装置、あるいは複数のグループに共有のデバイスキーであるノードキーを記憶している。さらに、記録再生装置の電子透かし世代情報を格納している。電子透かし世代情報については後段で詳細に説明する。

ＣＰＵ１７０は、メモリ１８０に記憶されたプログラムを実行することで、ＭＰＥＧコーデック１３０や暗号処理手段１５０等を制御する。ＣＰＵ１７０は、後述する著作権情報の生成処理を暗号処理手段１５０他とともに実行する。メモリ１８０は、例えば、不揮発性メモリで、ＣＰＵ１７０が実行するプログラムや、ＣＰＵ１７０の動作上必要なデータを記憶する。また、メモリ１８０は、後述する入力ソースに応じた出力制限規則データを格納している。

ドライブ１９０は、デジタルデータを記録再生可能な記録媒体１９５を駆動す

ることにより、記録媒体１９５からデジタルデータを読み出し（再生し）、バス１１０上に出力するとともに、バス１１０を介して供給されるデジタルデータを、記録媒体１９５に供給して記録させる。また、プログラムをＲＯＭ１６０に、デバイスキーをメモリ１８０に記憶するようにしてもよい。

記録媒体１９５は、例えば、ＤＶＤ、ＣＤ等の光ディスク、光磁気ディスク、ＨＤ等の磁気ディスク、磁気テープ、あるいはＲＡＭ等の半導体メモリ等のデジタルデータの記憶可能な媒体であり、本実施の形態では、ドライブ１９０に対して着脱可能な構成であるとする。但し、記録媒体１９５は、記録再生装置１００に内蔵する構成としてもよい。

トランスポート・ストリーム処理手段（ＴＳ処理手段）３００は、後段において図を用いて詳細に説明するが、例えば複数のＴＶプログラム（コンテンツ）が多重化されたトランスポートストリームから特定のプログラム（コンテンツ）に対応するトランスポートパケットを取り出して、取り出したトランスポートストリームの出現タイミング情報を各パケットとともに記録媒体１９５に格納するためのデータ処理および、記録媒体１９５からの再生処理時の出現タイミング制御処理を行なう。

トランスポートストリームには、各トランスポートパケットの出現タイミング情報としてのＡＴＳ（Arrival Time Stamp：着信時刻スタンプ）が設定されており、このタイミングはＭＰＥＧ２システムズで規定されている仮想的なデコーダであるＴ－ＳＴＤ(Transport stream System Target Decoder)を破綻させないように符号化時に決定され、トランスポートストリームの再生時には、各トランスポートパケットに付加されたＡＴＳによって出現タイミングを制御する。トランスポート・ストリーム処理手段（ＴＳ処理手段）３００は、これらの制御を実行する。例えば、トランスポートパケットを記録媒体に記録する場合には、各パケットの間隔を詰めたソースパケットとして記録するが、各トランスポートパケットの出現タイミングを併せて記録媒体に保存することにより、再生時に各パケットの出力タイミングを制御することが可能となる。トランスポート・ストリーム処理手段（ＴＳ処理手段）３００は、ＤＶＤ等の記録媒体１９５へのデータ記録時に、各トランスポートパケットの入力タイミングを表すＡＴＳ（Arrival

Time Stamp：着信時刻スタンプ）を付加して記録する。

本発明の記録再生装置１００は、上述のＡＴＳの付加されたトランスポートストリームによって構成されるコンテンツについて、暗号処理手段１５０において暗号化処理を実行し、暗号化処理のなされたコンテンツを記録媒体１９５に格納する処理が可能である。さらに、暗号処理手段１５０は、記録媒体１９５に格納された暗号化コンテンツの復号処理を実行する。これらの処理の詳細については、後段で説明する。

電子透かし（ウォーターマーク（ＷＭ））検出、埋め込み手段１８５は、記録媒体に対する格納対象コンテンツ、あるいは記録媒体からの再生処理対象コンテンツに対応するコピー制御情報を電子透かしとして埋め込む処理を実行し、また埋め込まれた電子透かしの検出処理を実行する。なお、コピー制御情報の書き換え処理としての電子透かし埋め込み処理も実行する。これらの処理の詳細については、後段で説明する。

記録媒体１９５には、例えばディスクの製造時のスタンパー毎に設定されるスタンパーＩＤ、ディスク毎に異なって設定されるディスクＩＤ、コンテンツ毎に異なって設定するコンテンツＩＤ、あるいは暗号処理用のキー等、様々な識別データ、暗号処理鍵等の秘密情報が格納される。

記録媒体１９５に格納された各種の秘密情報は、それらが暗号化情報である場合は、暗号処理手段１５０において復号され、復号した情報を用いて記録媒体に対するコンテンツ記録、再生時に適用する暗号処理鍵を生成する。秘密情報は暗号処理手段１５０内で実行されるコンテンツ暗号化キー生成においてのみ使用される構成であり、秘密情報の外部への漏洩を防止した構成となっている。

なお、図１に示す暗号処理手段１５０、ＴＳ処理手段３００、電子透かし（ＷＭ）検出、埋め込み手段１８５は、理解を容易にするため、別ブロックとして示してあるが、各機能を実行する１つまたは複数のＬＳＩとして構成してもよく、また、各機能のいずれかをソフトウェアまたはハードウェアを組み合わせた構成によって実現する構成としてもよい。

本発明の記録再生装置の構成例としては図１に示す構成の他に図２に示す構成が可能である。図２に示す記録再生装置２００では、記録媒体２０５はドライブ

装置としての記録媒体インタフェース（Ｉ／Ｆ）２１０から着脱が可能であり、この記録媒体２０５を別の記録再生装置に装着してもデータの読み出し、書き込みが可能な構成としたものである。

［２．記録、再生処理］

次に、図１あるいは図２の記録再生装置における記録媒体に対するデータ記録処理および記録媒体からのデータ再生処理について、図３および図４のフローチャートを参照して説明する。外部からのデジタル信号のコンテンツを、記録媒体１９５に記録する場合においては、図３（Ａ），（Ｂ）のフローチャートにしたがった記録処理が行われる。図３（Ａ）は、企業５社の共同提案としての５Ｃ－ＤＴＣＰ（Digital Transmission Content Protection）システムで提唱するコピー制御情報(ＣＣＩ：Copy Control Information)によって保護されたデジタル信号処理を実行する場合の処理フローであり、図３（Ｂ）は、５Ｃ－ＤＴＣＰシステムで提唱するコピー制御情報(ＣＣＩ)によって保護されていないデジタル信号処理を実行する場合の処理フローである。

図３（Ａ）に示すフローについて説明する。デジタル信号のコンテンツ（デジタルコンテンツ）が、例えば、IEEE(Institute of Electrical and Electronics Engineers)1394 シリアルバス等を介して、入出力Ｉ／Ｆ１２２に供給されると、ステップＳ３０１において、入出力Ｉ／Ｆ１２０は、供給されるデジタルコンテンツを受信し、バス１１０を介して、ＴＳ処理手段３００に出力する。

ＴＳ処理手段３００は、ステップＳ３０２において、トランスポートストリームを構成する各トランスポートパケットにＡＴＳ（Arrival Time Stamp（着信時刻スタンプ））を付加したブロックデータを生成して、バス１１０を介して、暗号処理手段１５０に出力する。

暗号処理手段１５０は、ステップＳ３０３において、受信したデジタルコンテンツに対する暗号化処理を実行し、その結果として得られる暗号化コンテンツをバス１１０を介して、ドライブ１９０、あるいは記録媒体Ｉ／Ｆ２１０に出力する。暗号化コンテンツは、ドライブ１９０、あるいは記録媒体Ｉ／Ｆ２１０を介して記録媒体１９５に記録（Ｓ３０４）され、記録処理を終了する。なお、暗号処理手段１５０における暗号処理については後段で説明する。

なお、ＩＥＥＥ１３９４シリアルバスを介して接続した装置相互間で、デジタルコンテンツを伝送するときの、デジタルコンテンツを保護するための規格として、５ＣＤＴＣＰ(Five Company Digital Transmission Content Protection)が定められているが、このＤＴＣＰでは、コピーフリーでないデジタルコンテンツを装置相互間で伝送する場合、データ伝送に先立って、送信側と受信側が、コピーを制御するためのコピー制御情報（ＣＣＩ）を正しく取り扱えるかどうかの認証を相互に行い、その後、送信側において、デジタルコンテンツを暗号化して伝送し、受信側において、その暗号化されたデジタルコンテンツ（暗号化コンテンツ）を復号し、コピー制御情報（ＣＣＩ）に従った処理を実行し、コピー制御情報（ＣＣＩ）の更新処理を実行するようになっている。

ＤＴＣＰにより規定されたコピー制御情報（ＣＣＩ）は、トランポートパケットに対して例えば２ビット情報が付加され、その情報が付加されたデータは制限なくコピーが許可されていることを示すコピーフリー（Copy Free)、1 世代のみのコピーを許可する１世代コピー許可（One Generation Copy Allowed)、コピーを認めないコピー禁止（Copy Prohibited）などの情報を示す。具体的には、ＣＧＭＳ方式の場合、２ビットの情報の意味内容は、[００]……コピーフリー、[１０]……コピー１世代可、[１１]……コピー禁止となる。

記録再生装置がＤＴＣＰに準拠した装置である場合は、入力情報のＣＣＩに基づいて、コンテンツの格納（コピー）が可能か否かを判定し、判定に従った処理を実行する。例えば入力コンテンツに対して設定されたＣＣＩ：１１（コピー禁止）である場合は、コンテンツの記録媒体に対する格納処理は実行されないことになる。また、入力コンテンツに対して設定されたＣＣＩ：１０（コピー１世代可）である場合は、コンテンツの格納時にＣＣＩの書き換えを行ない、ＣＣＩ：１１（コピー禁止）として、コンテンツの格納処理を実行することになる。

また、ＤＴＣＰに規格に基づくデータ送受信においては、データ受信側の入出力Ｉ／Ｆ１２２は、ステップＳ３０１で、IEEE1394 シリアルバスを介して暗号化コンテンツを受信し、その暗号化コンテンツを、ＤＴＣＰ規格に準拠して復号し、平文のコンテンツとして、その後、暗号処理手段１５０に出力する。

ＤＴＣＰによるデジタルコンテンツの暗号化は、時間変化するキーを生成し、

そのキーを用いて行われる。暗号化されたデジタルコンテンツは、その暗号化に用いたキーを含めて、IEEE1394シリアルバス上を伝送され、受信側では、暗号化されたデジタルコンテンツを、そこに含まれるキーを用いて復号する。

なお、ＤＴＣＰによれば、正確には、キーの初期値と、デジタルコンテンツの暗号化に用いるキーの変更タイミングを表すフラグとが、暗号化コンテンツに含められる。そして、受信側では、その暗号化コンテンツに含まれるキーの初期値を、やはり、その暗号化コンテンツに含まれるフラグのタイミングで変更していくことで、暗号化に用いられたキーが生成され、暗号化コンテンツが復号される。但し、ここでは、暗号化コンテンツに、その復号を行うためのキーが含まれていると等価であると考えても差し支えないため、以下では、そのように考えるものとする。ここで、ＤＴＣＰについては、例えば、http://www.dtcp.com のURL(Uniform Resource Locator)で特定されるＷｅｂページにおいて概要情報が開示されている。

図３（Ｂ）に示すフローについて説明する。図３（Ｂ）のフローは、５Ｃ－ＤＴＣＰシステムで提唱するコピー制御情報(ＣＣＩ)によって保護されていないデジタル信号処理を実行する場合の処理フローであり、デジタル信号のコンテンツ（デジタルコンテンツ）が、例えば、ＵＳＢ等を介して入出力Ｉ／Ｆ１２１に供給、あるいはＩＥＥＥ１３９４バスを介して入出力Ｉ／Ｆ１２２に供給されると、ステップＳ３１１において、供給されるデジタルコンテンツを受信し、バス１１０を介して、電子透かし検出、埋め込み手段１８５に出力する。

電子透かし検出、埋め込み手段１８５は、入力コンテンツに埋め込まれている電子透かしとしてのコピー制御情報を検出し、コピー制御情報に従った処理を実行する。電子透かし（ＷＭ：Watermark）は、まずコンテンツが製作されるときに、もともとのコンテンツのコピー情報としてプライマリ・マーク（Primary Mark）がコンテンツに埋め込まれる。これはたとえば、１１（コピー禁止)、１０（１世代コピー可)、００（コピーフリー）の２ビット情報である。記録装置がコピーを作る際には、１０のプライマリ・マークに対して、コピーマーク（Copy Mark）と呼ばれる１ビットの値１を付加し、１０１という値にしてコンテンツに対して電子透かしの再埋め込みを実行することにより、コンテンツがコピーであることを

示す。プライマリ・マークが００（コピーフリー）の場合にはコピーマークを付加する必要がなく、１１（コピー禁止）の場合にはコピー禁止であるので記録機器はコピーを作らない。このように電子透かしとして埋め込まれたコピー制御情報に従ってコンテンツの記録を行なう。

ただし、電子透かしの処理可能な機器と不可能な機器が存在する。これらは例えば３つの世代の機器として、下記のように区分される。

第１世代：電子透かしの検出、埋め込みを実行しない機器。

第２世代：検出のみが可能な機器（プライマリ・マーク検出は可能、コピー・マーク付加処理は不可能）。

第３世代：検出、埋め込み可能な機器（プライマリ・マーク、コピー・マーク付加処理が可能）。

これらの機器において、実行される処理は、それぞれ異なることになる。これらの処理の具体的態様については、後段で説明する。

図３（Ｂ）のフローの説明を続ける。電子透かしの処理がステップＳ３１２で実行されると、ステップＳ３１３において、ＴＳ処理手段３００に出力する。

ＴＳ処理手段３００における処理には、記録媒体に格納するトランスポートストリームデータに対するコピー制御情報（ＣＣＩ）の設定処理が含まれることになるが、図３（Ｂ）の入力データは、ＣＣＩの制御を実行していないデジタル信号であり、入力データに付加されているＣＣＩは信用できない可能性がある。この場合、前述のステップＳ３１２の電子透かし処理において検出した電子透かしに基づくコピー制御情報に基づいて、新たなＣＣＩ設定が記録媒体に格納するトランスポートストリームデータに対して実行される。

すなわち、ＣＣＩ非保護データを入力した場合は、入力情報の電子透かしに基づいて、コンテンツの格納（コピー）が可能か否かを判定し、判定に従った処理を実行する。例えば入力コンテンツに対して埋め込まれた電子透かしが１１（コピー禁止）である場合は、コンテンツの記録媒体に対する格納処理は実行されないことになる。また、入力コンテンツに対して設定された電子透かしが１０（コピー１世代可）である場合は、ＴＳ処理手段３００において、コンテンツの格納時にＣＣＩを１１（コピー禁止）として、コンテンツの格納処理を実行すること

になる。

このように、ＣＣＩ非保護データの処理においては、電子透かし（ＷＭ）に基づいてトランスポートストリーム中のＣＣＩが設定されることになる。

以下のステップＳ３１４，Ｓ３１５の処理は、図３（Ａ）のＳ３０３，Ｓ３０４と同様の処理である。なお、電子透かしの埋め込み可能な機器においては、更新されたコピー制御情報を電子透かしとして埋め込んだコンテンツが記録媒体に格納されることになる。

次に、外部からのアナログ信号のコンテンツを、記録媒体１９５に記録する場合の処理について、図３（Ｃ）のフローチャートに従って説明する。アナログ信号のコンテンツ（アナログコンテンツ）が、入出力Ｉ／Ｆ１４０に供給されると、入出力Ｉ／Ｆ１４０は、ステップＳ３２１において、そのアナログコンテンツを受信し、ステップＳ３２２に進み、内蔵するＡ／Ｄ，Ｄ／Ａコンバータ１４１でＡ／Ｄ変換して、デジタル信号のコンテンツ（デジタルコンテンツ）とする。

このデジタルコンテンツは、ＭＰＥＧコーデック１３０に供給され、ステップＳ３２３において、ＭＰＥＧエンコード、すなわちＭＰＥＧ圧縮による符号化処理が実行され、バス１１０を介して、暗号処理手段１５０に供給される。

以下、ステップＳＳ３２４、Ｓ３２５、Ｓ３２６において、図３（Ｂ）のステップＳ３１２、Ｓ３１３、Ｓ３１４における処理と同様の処理が行われる。すなわち、電子透かし検出、埋め込み手段１８５による電子透かしの検出、更新、ＴＳ処理手段３００によるトランスポートパケットに対するＡＴＳ付加、検出電子透かしに基づくＣＣＩ（コピー制御情報）付加、暗号処理手段１５０における暗号化処理が実行され、その結果得られる暗号化コンテンツを、記録媒体１９５に記録して、記録処理を終了する。

上述したように、本発明の情報処理装置としての記録再生装置におけるコンテンツの記録処理は、そのコンテンツの入力ソースによって変更して実行される。５ＣＤＴＣＰを用いたＩＥＥＥ１３９４からのコンテンツ入力の場合や、衛星・地上波のデジタルテレビ放送など、そのコンテンツのコピー制御情報（ＣＣＩ）を送信する方法が規定されており、またその情報が保護されている場合には、それに基づいて記録コンテンツのＣＣＩを判断する。これに対し、５ＣＤＴＣＰに

よりコンテンツやＣＣＩを保護していないＩＥＥＥ１３９４入力や、アナログ入力においては、そのコンテンツのＣＣＩを定めるために、入力されたコンテンツの電子透かしを、記録処理中ずっと検出しつづける必要がある。この結果、確定したＣＣＩによっては、記録を停止する処理を実行する場合がある。すなわち、電子透かし検出情報から取得されるコピー制御情報がコピー禁止であった場合などには、コンテンツを記録しない。

なお、本発明の記録再生装置においては、コンテンツの記録に際して著作権情報（Copyright Information）を、格納コンテンツに対応付けて記録媒体に記録する。格納する著作権情報（Copyright Information）は、例えば、入力ソース情報、記録機器の電子透かし世代情報（前述の第１、２，３世代）、後述する記録モードの各情報、コンテンツ中から取得されるコピー制御情報としてのＣＣＩから選択された最も厳しい最厳格コピー制御情報(タイトル別コピー制御情報)、さらに、記録コンテンツにおけるコピー制御情報の変化点を示す情報としての対応パケットナンバーと変化点におけるコピー制御情報などであり、これらの情報中から１以上の情報を著作権情報として設定して記録媒体に格納する。これらの情報の詳細、および格納処理例については後述する。

タイトル別コピー制御情報について説明する。コンテンツ中には、一般に様々なデータが混在しており、コピー禁止の部分や、コピーフリーの部分、コピー１世代可として設定した部分が混在する。これらの検出された様々なコピー制御情報から最も制限の厳しいものとして選択された最厳格コピー制御情報をタイトル別コピー制御情報として設定し、コンテンツに対応付けて記録媒体に格納する。なお、本発明の記録再生装置においては、記録媒体に格納するコンテンツにはコンテンツに対応して設定されるタイトル毎に生成される暗号処理鍵としてのタイトルキーがコンテンツに対応付けられて記録媒体に格納され、タイトルキーを用いた暗号処理が実行される。これらの処理については、後述する。

なお、制限の厳しいコピー制御情報は、例えばコピー禁止、１世代コピー可、コピーフリーの順である。１つのタイトルキーに対応付けられて記録媒体に格納される記録対象コンテンツに例えば、１世代コピー可、コピーフリーの２つのコピー制御情報が含まれる場合には、タイトル別コピー制御情報として［１世代コ

ピー可］が設定される。コピー禁止が含まれる場合には［コピー禁止］が設定されることになる。コピーフリーのみの場合に限り、タイトル別コピー制御情報として［コピーフリー］が設定されることになる。

次に、記録媒体１９５に記録されたコンテンツを再生して、デジタルコンテンツ、あるいはアナログコンテンツとして出力する処理について図４のフローに従って説明する。再生時の処理は、その再生対象コンテンツに対応付けられて記録媒体に格納された著作権情報（Copyright Information）内の情報である入力ソース情報、すなわちどの入力ソースから来たコンテンツかの情報に応じて、また、タイトル別コピー制御情報が記録されているかに応じて変更される。

まず、タイトル別コピー制御情報が記録されている場合には、それに基づいてコンテンツのコピー制御態様としての処理態様を判断し、再生してよいかどうかを決める。タイトル別コピー制御情報が記録されていない場合には、電子透かしを検出しながら再生処理を行い、その結果に応じて再生してよいかどうかを決める。そして、再生してよいという場合には、入力ソースによって、それぞれの入力ソースで決められたルールに従った形態で出力を行う。一般的には、コンテンツがコピーフリーでない場合には、出力時にコンテンツを保護する必要がある。デジタル出力の場合は、たとえば５ＣＤＴＤＰの規定に従ってトランスポートストリームに対するＣＣＩ設定を行ないながら出力し、アナログ出力の場合には、たとえばマクロビジョン（Macrovision）信号をコンテンツに付加しながら出力する。映像信号の場合、例えば、ＣＧＭＳ方式の付加情報（以下、ＣＧＭＳ情報という。）や、ＡＧＣの方式の相違を利用して、複製された映像信号の正常な利用を不能にするためのＡＧＣパルス信号（マクロビジョン方式の複製防止用の擬似同期信号）を付加して出力する。

図４（Ａ）の処理フローは、ＣＣＩ保護入力ソースから入力されたデータを記録媒体に格納した場合の記録データを記録媒体から再生して出力する処理の手順を示している。

まず最初に、ステップＳ４０１において、ドライブ１９０または記録媒体Ｉ／Ｆ２１０によって、記録媒体１９５に記録された暗号化コンテンツおよび、暗号化コンテンツに対応する著作権情報が読み出される。著作権情報中には、前述し

たように、入力ソース情報、記録機器の電子透かし世代情報、後述する記録モードの各情報、コンテンツ中から取得されるコピー制御情報としてのＣＣＩから選択された最も厳しい最厳格コピー制御情報としてのタイトル別コピー制御情報、さらに、記録コンテンツにおけるコピー制御情報の変化点を示す情報としての対応パケットナンバーと変化点におけるコピー制御情報の少なくとも１以上の情報が格納され、これらの情報に基づいてコンテンツの再生、出力の可否が判定される。これらの処理については、後述する。再生出力可である場合は、暗号化コンテンツは、バス１１０を介して、暗号処理手段１５０に出力される。

暗号処理手段１５０では、ステップＳ４０２において、ドライブ１９０または記録媒体Ｉ／Ｆ２１０から供給される暗号化コンテンツの復号処理が実行され、復号データがバス１１０を介して、ＴＳ処理手段３００に出力される。

ＴＳ処理手段３００は、ステップＳ４０３において、トランスポートストリームを構成する各トランスポートパケットのＡＴＳから出力タイミングを判定し、ＡＴＳに応じた制御を実行して、バス１１０を介して、入出力Ｉ／Ｆ１２０に供給する。また、トランスポートストリーム中のコピー制御情報（ＣＣＩ）を検出して、ＣＣＩに基づく制御を行なう。

ステップＳ４０４では、出力形態がアナログデあるか、デジタルであるかを判定し、デジタル出力であれば、デジタル入出力Ｉ／Ｆ１２１，１２２を介して、ＴＳ処理手段３００からのデジタルコンテンツを、外部に出力し、再生処理を終了する。なお、ＴＳ処理手段３００の処理、暗号処理手段１５０におけるデジタルコンテンツの復号処理については後述する。

なお、入出力Ｉ／Ｆ１２０は、ステップＳ４０５で、IEEE1394シリアルバスを介してデジタルコンテンツを出力する場合には、ＤＴＣＰの規格に準拠して、上述したように、相手の装置との間で認証を相互に行い、その後、デジタルコンテンツを暗号化して伝送する。

アナログコンテンツとして出力する場合には、暗号処理手段１５０において得られた復号されたデジタルコンテンツは、バス１１０を介して、ＭＰＥＧコーデック１３０に供給される。

ステップＳ４０６において、ＭＰＥＧコーデック１３０でデジタルコンテンツ

がＭＰＥＧデコード、すなわち伸長処理され、入出力Ｉ／Ｆ１４０に供給される。入出力Ｉ／Ｆ１４０は、ステップＳ４０７において、ＭＰＥＧコーデック１３０でＭＰＥＧデコードされたデジタルコンテンツを、内蔵するＡ／Ｄ，Ｄ／Ａコンバータ１４１でＤ／Ａ変換（Ｓ４２５）して、アナログコンテンツとする。そして、ステップＳ４０８に進み、入出力Ｉ／Ｆ１４０は、そのアナログコンテンツを、外部に出力し、再生処理を終了する。

一方、図４（Ｂ）の処理フローは、ＣＣＩ非保護入力ソースから入力されたデータを記録媒体に格納した場合の記録データを記録媒体から再生して出力する処理の手順を示している。この場合は、トランスポートストリーム中のブロックデータに付加されたＣＣＩではなく、コンテンツの電子透かしを検出して取得されるコピー制御情報に基づく再生制御を実行する。

図４（Ｂ）の処理フローでは、ＴＳ処理（Ｓ４１３）の後のステップとしてステップＳ４１４の電子透かし（ＷＭ）処理がある点が（Ａ）に示す処理と異なる。この電子透かし（ＷＭ）処理は、再生コンテンツのデータ中の電子透かしを検出し、電子透かしからコピー制御情報を読み取り、読み取った電子透かしに基づいて再生制御を行なう処理である。例えばコピー禁止を示す電子透かしが検出された場合は、外部出力を伴う再生は実行しないなどの制御がなされる。

本発明の記録再生装置においては、上述したように、記録媒体に対するコンテンツの記録に際して著作権情報（Copyright Information）が記録媒体に格納され、再生時には、再生対象コンテンツに対応する著作権情報（Copyright Information）が取得されて著作権情報中の各種情報に従った制御がなされる。これらの処理については、後段で説明する。

［３．トランスポートストリーム（ＴＳ）処理］

次に、図５以下を用いて、本発明における記録媒体上のデータフォーマットを説明する。ここで説明するデータフォーマットは、例えばＤＶＲシステムにおいてメデイアに格納されるデータ・フォーマットである。以下、記録媒体上のデータの読み書きの最小単位をブロック(block)という名前で呼ぶ。１ブロックは、１９２＊Ｘ（エックス）バイト（例えばＸ＝３２）の大きさとなっている。

本発明では、ＭＰＥＧ２のＴＳ（トランスポート・ストリーム）パケット（１

８８バイト）にＡＴＳを付加して１９２バイトとして、それをＸ個集めて１ブロックのデータとしている。ＡＴＳは２４乃至３２ビットの着信時刻を示すデータであり、先にも説明したようにArrival Time Stamp（着信時刻スタンプ）の略である。ＡＴＳは各パケットの着信時刻に応じたランダム性のあるデータとして構成される。記録媒体のひとつのブロック（セクタ）には、ＡＴＳを付加したＴＳ（トランスポート・ストリーム）パケットをＸ個記録する。本発明の構成では、トランスポートストリームを構成する各ブロックの第１番目のＴＳパケットに付加されたＡＴＳを用いてそのブロック（セクタ）のデータを暗号化するブロックキーを生成する。

ランダム性のあるＡＴＳを用いて暗号化用のブロックキーを生成することにより、ブロック毎に異なる固有キーが生成される。生成されたブロック固有キーを用いてブロック毎の暗号化処理を実行する。また、ＡＴＳを用いてブロックキーを生成する構成とすることにより、各ブロック毎の暗号化鍵を格納するための記録媒体上の領域が不要となり、メインデータ領域が有効に使用可能となる。さらに、データの記録、再生時にメインデータ部以外のデータをアクセスする必要もなくなり、処理が効率的になる。

なお、図５に示すブロック・シード（Block Seed）は、ＡＴＳを含む付加情報である。ブロック・シードは、さらにＡＴＳだけでなくコピー制御情報(ＣＣＩ：Copy Control Information)も付加される。この場合、ＡＴＳとＣＣＩを用いてブロックキーを生成する構成とすることができる。

なお、ここで、ブロック・シードに含まれるコピー制限情報(ＣＣＩ：Copy Control Information)は、前述した５Ｃ ＤＴＣＰ(Digital Transmission Content Protection）システムで提唱するコピー制御情報（ＣＣＩ：Copy Control Information）であり、デバイスの能力に応じた２種類の情報、すなわち、ＥＭＩ（Encryption Mode Indicator)、あるいは、コピー制御情報を送るための場所があらかじめ確保されているようなフォーマットにおいて適用されるコンテンツに埋め込まれたコピー制御情報（ＣＣＩ）である埋め込みＣＣＩ（Embedded CCI）のいずれかの情報を反映したものとなる。

なお、本発明の構成においては、ＤＶＤ等の記録媒体上にデータを格納する場

合、コンテンツの大部分のデータは暗号化されるが、図５の最下段に示すように、ブロックの先頭のｍ（たとえば、ｍ＝８または１６）バイトは暗号化されずに平文（Unencrypted data）のまま記録され、残りのデータ（ｍ＋１バイト以降）が暗号化される。これは暗号処理が８バイト単位としての処理であるために暗号処理データ長（Encrypted data）に制約が発生するためである。なお、もし、暗号処理が８バイト単位でなく、たとえば１バイト単位で行なえるなら、ｍ＝４として、ブロックシード以外の部分をすべて暗号化してもよい。

ここで、ＡＴＳの機能について詳細に説明する。ＡＴＳは、先にも説明したように入力トランスポートストリーム中の各トランスポートパケットの出現タイミングを保存するために付加する着信時刻スタンプである。

すなわち、例えば複数のＴＶプログラム（コンテンツ）が多重化されたトランスポートストリームの中から１つまたは幾つかのＴＶプログラム（コンテンツ）を取り出した時、その取り出したトランスポートストリームを構成するトランスポートパケットは、不規則な間隔で現れる（図７（ａ）参照)。トランスポートストリームは、各トランスポートパケットの出現タイミングに重要な意味があり、このタイミングはＭＰＥＧ２システムズ（ＩＳＯ／ＩＥＣ １３８１８－１）で規定されている仮想的なデコーダであるＴ－ＳＴＤ(Transport stream System Target Decoder)を破綻させないように符号化時に決定される。

トランスポートストリームの再生時には、各トランスポートパケットに付加されたＡＴＳによって出現タイミングが制御される。従って、記録媒体にトランスポートパケットを記録する場合には、トランスポートパケットの入力タイミングを保存する必要があり、トランスポートパケットをＤＶＤ等の記録媒体に記録する時に、各トランスポートパケットの入力タイミングを表すＡＴＳを付加して記録する。

図６に、デジタルインタフェース経由で入力されるトランスポートストリームをＤＶＤ等の記録媒体であるストレージメディアに記録する時のＴＳ処理手段３００において実行する処理を説明するブロック図を示す。端子６００からは、デジタル放送等のデジタルデータとしてトランスポートストリームが入力される。図１または図２においては、入出力Ｉ／Ｆ１２０を介して、あるいは入出力Ｉ／

Ｆ１４０、ＭＰＥＧコーデック１３０を介して端子６００からトランスポートストリームが入力される。

トランスポートストリームは、ビットストリームパーサー(parser)６０２に入力される。ビットストリームパーサー６０２は、入力トランスポートストリームの中からＰＣＲ(Program Clock Reference)パケットを検出する。ここで、ＰＣＲパケットとは、ＭＰＥＧ２システムズで規定されているＰＣＲが符号化されているパケットである。ＰＣＲパケットは、１００ｍｓｅｃ以内の時間間隔で符号化されている。ＰＣＲは、トランスポートパケットが受信側に到着する時刻を２７ＭＨｚの精度で表す。

そして、２７ＭＨｚＰＬＬ６０３において、記録再生器が持つ２７ＭＨｚクロックをトランスポートストリームのＰＣＲにロック（Lock）させる。タイムスタンプ発生回路６０４は、２７ＭＨｚクロックのクロックのカウント値に基づいたタイムスタンプを発生する。そして、ブロック・シード（Block seed）付加回路６０５は、トランスポートパケットの第１バイト目がスムージングバッファ６０６へ入力される時のタイムスタンプをＡＴＳとして、そのトランスポートパケットに付加する。

ＡＴＳが付加されたトランスポートパケットは、スムージングバッファ６０６を通って、端子６０７から、暗号処理手段１５０に出力され、後段で説明する暗号処理が実行された後、ドライブ１９０（図１）、記録媒体Ｉ／Ｆ２１０（図２）を介してストレージメディアである記録媒体１９５に記録される。

図７は、入力トランスポートストリームが記録媒体に記録される時の処理の例を示す。図７（ａ）は、ある特定プログラム（コンテンツ）を構成するトランスポートパケットの入力を示す。ここで横軸は、ストリーム上の時刻を示す時間軸である。この例ではトランスポートパケットの入力は、図７（ａ）に示すように不規則なタイミングで現れる。

図７（ｂ）は、ブロック・シード（Block Seed）付加回路６０５の出力を示す。ブロック・シード（Block Seed）付加回路６０５は、トランスポートパケット毎に、そのパケットのストリーム上の時刻を示すＡＴＳを含むブロック・シード（Block Seed）を付加して、ソースパケットを出力する。図７（ｃ）は記録媒体

に記録されたソースパケットを示す。ソースパケットは、図７（ｃ）に示すように間隔を詰めて記録媒体に記録される。このように間隔を詰めて記録することにより記録媒体の記録領域を有効に使用できる。

図８は、記録媒体１９５に記録されたトランスポートストリームを再生する場合のＴＳ処理手段３００の処理構成ブロック図を示している。端子８００からは、後段で説明する暗号処理手段において復号されたＡＴＳ付きのトランスポートパケットが、ブロック・シード（Block seed）分離回路８０１へ入力され、ＡＴＳとトランスポートパケットが分離される。タイミング発生回路８０４は、再生器が持つ２７ＭＨｚクロック８０５のクロックカウンター値に基づいた時間を計算する。

なお、再生の開始時において、一番最初のＡＴＳが初期値として、タイミング発生回路８０４にセットされる。比較器８０３は、ＡＴＳとタイミング発生回路８０４から入力される現在の時刻を比較する。そして、タイミング発生回路８０４が発生する時間とＡＴＳが等しくなった時、出力制御回路８０２は、そのトランスポートパケットをＭＰＥＧコーデック１３０またはデジタル入出力Ｉ／Ｆ１２０へ出力する。

図９は、入力ＡＶ信号を記録再生器１００のＭＰＥＧコーデック１３０においてＭＰＥＧエンコードして、さらにＴＳ処理手段３００においてトランスポートストリームを符号化する構成を示す。従って図９は、図１または、図２おけるＭＰＥＧコーデック１３０とＴＳ処理手段３００の両処理構成を併せて示すブロック図である。端子９０１からは、ビデオ信号が入力されており、それはＭＰＥＧビデオエンコーダ９０２へ入力される。

ＭＰＥＧビデオエンコーダ９０２は、入力ビデオ信号をＭＰＥＧビデオストリームに符号化し、それをバッファビデオストリームバッファ９０３へ出力する。また、ＭＰＥＧビデオエンコーダ９０２は、ＭＰＥＧビデオストリームについてのアクセスユニット情報を多重化スケジューラ９０８へ出力する。ビデオストリームのアクセスユニットとは、ピクチャであり、アクセスユニット情報とは、各ピクチャのピクチャタイプ，符号化ビット量，デコードタイムスタンプである。ここで、ピクチャタイプは、Ｉ／Ｐ／Ｂピクチャ（picture）の情報である。また、

デコードタイムスタンプは、ＭＰＥＧ２システムズで規定されている情報である。

端子９０４からは、オーディオ信号が入力されており、それはＭＰＥＧオーディオエンコーダ９０５へ入力される。ＭＰＥＧオーディオエンコーダ９０５は、入力オーディオ信号をＭＰＥＧオーディオストリームに符号化し、それをバッファ９０６へ出力する。また、ＭＰＥＧオーディオエンコーダ９０５は、ＭＰＥＧオーディオストリームについてのアクセスユニット情報を多重化スケジューラ９０８へ出力する。オーディオストリームのアクセスユニットとは、オーディオフレームであり、アクセスユニット情報とは、各オーディオフレームの符号化ビット量，デコードタイムスタンプである。

多重化スケジューラ９０８には、ビデオとオーディオのアクセスユニット情報が入力される。多重化スケジューラ９０８は、アクセスユニット情報に基づいて、ビデオストリームとオーディオストリームをトランスポートパケットに符号化する方法を制御する。多重化スケジューラ９０８は、内部に２７ＭＨｚ精度の基準時刻を発生するクロックを持ち、そして、ＭＰＥＧ２で規定されている仮想的なデコーダモデルであるＴ－ＳＴＤを満たすようにして、トランスポートパケットのパケット符号化制御情報を決定する。パケット符号化制御情報は、パケット化するストリームの種類とストリームの長さである。

パケット符号化制御情報がビデオパケットの場合、スイッチ９７６はａ側になり、ビデオストリームバッファ９０３からパケット符号化制御情報により指示されたペイロードデータ長のビデオデータが読み出され、トランスポートパケット符号化器９０９へ入力される。

パケット符号化制御情報がオーディオパケットの場合、スイッチ９７６はｂ側になり、オーディオストリームバッファ９０６から指示されたペイロードデータ長のオーディオデータが読み出され、トランスポートパケット符号化器９０９へ入力される。

パケット符号化制御情報がＰＣＲパケットの場合、トランスポートパケット符号化器９０９は、多重化スケジューラ９０８から入力されるＰＣＲを取り込み、ＰＣＲパケットを出力する。パケット符号化制御情報がパケットを符号化しないことを指示する場合、トランスポートパケット符号化器９０９へは何も入力され

ない。

トランスポートパケット符号化器９０９は、パケット符号化制御情報がパケットを符号化しないことを指示する場合、トランスポートパケットを出力しない。それ以外の場合、パケット符号化制御情報に基づいてトランスポートパケットを生成し、出力する。したがって、トランスポートパケット符号化器９０９は、間欠的にトランスポートパケットを出力する。到着(Arrival)タイムスタンプ(time stamp)計算手段９１０は、多重化スケジューラ９０８から入力されるＰＣＲに基づいて、トランスポートパケットの第１バイト目が受信側に到着する時刻を示すＡＴＳを計算する。

多重化スケジューラ９０８から入力されるＰＣＲは、ＭＰＥＧ２で規定されるトランスポートパケットの１０バイト目の受信側への到着時刻を示すので、ＡＴＳの値は、ＰＣＲの時刻から１０バイト前のバイトが到着する時刻となる。

ブロック・シード（Block Seed）付加回路９１１は、トランスポートパケット符号化器９０９から出力されるトランスポートパケットにＡＴＳを付加する。ブロック・シード（Block seed）付加回路９１１から出力されるＡＴＳ付きのトランスポートパケットは、スムージングバッファ９１２を通って、暗号処理手段１５０へ入力され、後段で説明する暗号処理が実行された後、ストレージメディアである記録媒体１９５へ格納される。

記録媒体１９５へ格納されるＡＴＳ付きのトランスポートパケットは、暗号処理手段１５０で暗号化される前に図７（ｃ）に示すように間隔を詰めた状態で入力され、その後、記録媒体１９５に格納される。トランスポートパケットが間隔を詰めて記録されても、ＡＴＳを参照することによって、そのトランスポートパケットの受信側への入力時刻を制御することができる。

ところで、ＡＴＳの大きさは３２ビットに決まっているわけではなく、２４ビット乃至３１ビットでも構わない。ＡＴＳのビット長が長いほど、ＡＴＳの時間カウンターが一周する周期が長くなる。例えば、ＡＴＳが２７ＭＨｚ精度のバイナリーカウンターである場合、２４－ｂｉｔ長のＡＴＳが一周する時間は、約0.6秒である。この時間間隔は、一般のトランスポートストリームでは十分な大きさである。なぜなら、トランスポートストリームのパケット間隔は、ＭＰＥＧ２の

規定により、最大０．１秒と決められているからである。しかしながら、十分な余裕を見て、ＡＴＳを２４－ｂｉｔ以上にしても良い。

このように、ＡＴＳのビット長を様々な長さとした場合、ブロックデータの付加データであるブロックシードの構成としていくつかの構成が可能となる。ブロック・シードの構成例を図１０に示す。図１０の例１は、ＡＴＳを３２ビット分使用する例である。図１０の例２は、ＡＴＳを３０ビットとし、コピー制御情報（ＣＣＩ）を２ビット分使用する例である。コピー制御情報は、それが付加されたデータのコピー制御の状態を表す情報であり、ＳＣＭＳ：Serial Copy Management System やＣＧＭＳ：Copy Generation Management System が有名である。これらのコピー制御情報では、その情報が付加されたデータは制限なくコピーが許可されていることを示すコピーフリー（Copy Free)、1 世代のみのコピーを許可する 1 世代コピー許可（One Generation Copy Allowed)、コピーを認めないコピー禁止（Copy Prohibited）などの情報が表せる。

図１０に示す例３は、ＡＴＳを２４ビットとし、ＣＣＩを２ビット使用し、さらに他の情報を 6 ビット使用する例である。他の情報としては、たとえばこのデータがアナログ出力される際に、アナログ映像データのコピー制御機構であるマクロビジョン（Macrovision）のオン／オフ（On/Off）を示す情報など、様々な情報を利用することが可能である。

［４．電子透かし（ＷＭ）処理］

次に、電子透かしによるコピー制御処理について説明する。電子透かし（ＷＭ：Watermark）は、コンテンツに電子透かしパターンを埋め込み、例えば同一の電子透かしパターンとの相関値に基づいて電子透かしの有無を検出し、検出に応じてビット情報を取得するものである。検出されるビット情報に従って、コピーフリー、コピー１世代可、コピー禁止等の制御情報が示される。電子透かしによるコピー制御情報は、アナログ領域においてもコピー情報を残すことが可能であり、Ｄ／Ａ，Ａ／Ｄ変換がなされてもコピー制御情報を伝達することが可能となる。

電子透かしを用いたコピー制御情報の設定処理について説明する。まずコンテンツが製作されるときに、もともとのコンテンツのコピー制御情報としてプライマリマーク（Primary Mark）がコンテンツに埋め込まれる。これはたとえば、２

ビット情報であり、１１（コピー禁止）、１０（１世代コピー可）、００（コピーフリー）である。そして、記録装置がコピーを作る際には、１０（１世代コピー可）のプライマリマーク（Primary Mark）の付加されたコンテンツを記録する場合は、１０に対して、コピーマーク（Copy Mark）と呼ばれる１ビットの値１を付加し、１０１という値にして、電子透かしの再埋め込みを行なって記録媒体に記録する。この処理により、記録媒体に格納されたコンテンツはコピーであることが示される。プライマリマーク（Primary Mark）が００の場合にはコピーマーク（Copy Mark）を付加する必要がなく、１１の場合にはコピー禁止であるので記録機器はコピーを作らない。

また、電子透かし（ＷＭ）は、上記のようなコピー制限のみでなく、再生制限にも用いられ得る。すなわち、ユーザ書き込み可能（user writable）なディスク上に、もともとコピー禁止を示す１１という情報を電子透かしとして埋め込まれたコンテンツがあったら、その再生をしない、という制御を実行することが可能である。また、サービス体系によっても異なるが、ユーザ書き込み可能（user writable）なディスク上にもともと１世代コピー可を示す１０というコピー情報を持つコンテンツを記録した場合には、上記のように コピーマーク（Copy Mark）が付加されて１０１というコピー情報とした電子透かしを埋め込むことが通常なので、１世代コピー可を示す１０というコピー情報を持つコンテンツが、ユーザ書き込み可能（user writable）なディスク上にあった場合にそれを再生しないように制限する構成とすることも可能である。

ところが、この電子透かしによるコピー制御情報の取り扱い方式は、コンテンツの態様によって様々な方式が提案されており、動画コンテンツに限っても多数の方式がある。現時点では広く規格化もしくはデファクトスタンダード化されているものはまだない。現時点での業界動向を鑑みるに、初期にはプライマリマーク（Primary Mark）のみが規格化もしくはデファクトスタンダード化され、その後にコピーマーク（Copy Mark）も含められると考えられる。つまり、現時点から将来に渡って、電子透かし（Watermak）の方式が定まるにつれてそれに対応した製品が市場にでると予測される。

すなわち、記録再生装置は電子透かし（ＷＭ：Watermark）の対応について、前

述したように次の３つの世代に分けられる。

第１世代：電子透かし（ＷＭ）の対応をしない。（検出、付加ともにしない）

第２世代：プライマリマーク（Primary Mark）のみ対応する。（検出はできるが付加はできない）第２世代機器におけるデータ記録時の具体的制御は下記のようになる。

記録時：記録されるコンテンツの電子透かしを検出する。

１１（コピー禁止）のコンテンツ：記録しない

１０（コピー１世代可）のコンテンツ：記録する。電子透かしは更新せずそのまま。

００（コピーフリー）のコンテンツ：記録する。電子透かしは更新せずそのまま。

第２世代機器におけるデータ再生時の具体的制御は下記のようになる。

再生時：ユーザ書き込み可能（user writable）なディスク上記録されている、再生するコンテンツの電子透かしを検出する。

１１（コピー禁止）のコンテンツ：再生しない。

１０（コピー１世代可）のコンテンツ：再生する。

００（コピーフリー）のコンテンツ：再生する。

第３世代：コピーマーク（Copy Mark）も含めて対応する。（検出、付加ともにできる）第３世代機器におけるデータ記録時の具体的制御は下記のようになる。

記録時：記録されるコンテンツの電子透かしを検出する。

１１（コピー禁止）のコンテンツ：記録しない

１０（コピー１世代可）のコンテンツ：記録する。電子透かしを１０１（それ以上コピー禁止）に更新（電子透かしの再書き込み）処理を実行する。

００（コピーフリー）のコンテンツ：記録する。電子透かしはそのまま。

１０１（それ以上コピー禁止）のコンテンツ：記録しない。

第３世代機器におけるデータ再生時の具体的制御は下記のようになる。

再生時：ユーザ書き込み可能（user writable）なディスク上に記録されている、再生するコンテンツの電子透かしを検出する。

１１（コピー禁止）のコンテンツ：再生しない。

１０（コピー１世代可）のコンテンツ：再生しない。

００（コピーフリー）のコンテンツ：再生する。

１０１（それ以上コピー禁止）のコンテンツ：再生する。

各世代の記録再生装置の基本的な記録再生のルールは上記のようになる。ところがこのような処理が行なわれた場合、ある世代の機器で記録したコンテンツを他の世代の機器で再生したようとしたとき、電子透かしとして記録されたコピー制御情報に従った正確な処理が行われない場合がある。例えば、第２世代の機器が１０（コピー１世代可）のプライマリマーク（Primary Mark）を持つコンテンツを記録した媒体を第３世代の機器で再生しようとすると、第３世代の機器の再生ルールに基づいて、このコンテンツの再生が行えなくなってしまう。

［５．著作権情報］

本発明は、上記問題のようなコピー制御処理における誤った処理を防止するものであり、記録媒体に対するコンテンツ格納処理の際に、著作権情報（Copyright Information）を記録媒体に記録し、再生時に著作権情報を参照し、著作権情報中に格納された各種の情報に基づいて制御を行なう。著作権情報（Copyright Information）には、コンテンツの入力ソース情報、記録機器の電子透かし世代情報（前述の第１、２，３世代）、記録モードの各情報と、コンテンツ中から取得されるコピー制御情報であるＣＣＩから選択された最も厳しい最厳格コピー制御情報としてのタイトル別コピー制御情報、さらに、記録コンテンツにおけるコピー制御情報の変化点を示す情報としての対応パケットナンバーと変化点におけるコピー制御情報などがあり、これらの情報中から１以上の情報を著作権情報として設定して記録媒体に格納する。著作権情報（Copyright Information）は、容易に改ざんされないように、正当性検査コードとしてのＭＡＣ（Message Authentication Code）が付加されて記録媒体に格納する。本発明の情報処理装置としての記録再生装置では、コンテンツの記録に際し、コンテンツに対応付けた著作権情報を生成して記録媒体に格納し、コンテンツ再生時には、コンテンツに対応して格納した著作権情報のＭＡＣ検証の後、改竄がないことが確認された著作権情報に従った再生、出力制御を行なう。

（１）電子透かし世代情報

著作権情報（Copyright Information）に含まれ得る各情報について説明する。電子透かしの世代情報については、上述した第１世代、第２世代、第３世代の情報であり、コンテンツを記録する記録装置内のＲＯＭに電子透かし世代情報が格納され、著作権情報生成時には、ＲＯＭから電子透かし世代情報を取得して、著作権情報中に格納する。

コンテンツの再生時に著作権情報内の電子透かし世代情報を取得して、記録機器の世代を確認することで、データ出力時の誤ったコピー制御を防止することが可能となる。具体的には、例えば、第２世代の機器が１０（コピー１世代可）のプライマリマーク（Primary Mark）を持つコンテンツを記録した媒体を第３世代の機器で再生しようとした場合、第３世代の機器は、再生コンテンツに対応する著作権情報を読み出し、著作権情報に格納された電子透かし世代情報に基づいて、コンテンツが第２世代の機器において記録されたコンテンツであることを確認する。第２世代の機器では、電子透かしの書き込みが実行されないことから、プライマリマーク（１０）がそのままの形で電子透かしとして残存していることが確認される。従って、第３世代の機器における再生処理は、コンテンツに格納された電子透かし制御情報（１０）は、第３世代における制御コードとしての１０１に対応するコードであると判断し、再生が可能となる。このようにコンテンツ記録機器の電子透かし世代情報をコンテンツ記録時に著作権情報として格納することにより、再生処理において、記録機器における世代に応じた正しい処理が可能となる。

（２）入力ソース情報

次に著作権情報として格納される入力ソース情報について説明する。入力ソース情報とは、記録対象コンテンツの入力ソースを示すものであり、例えば前述した５ＣＤＴＣＰに準拠した入力ソースからのコンテンツであるか、ＢＳ，ＣＳ等の衛星配信コンテンツであるか、地上波デジタルコンテンツであるか、地上波アナログコンテンツであるかなどの入力ソース情報である。

入力ソース情報としては、ＩＥＥＥ１３９４インタフェースを介するコピー制御情報を持つコンテンツ入力であるか否かを示す情報が含まれ、また、デジタルデータ入力であるかアナログデータ入力であるかを示す情報等が含まれる。これ

らは、データ入力を行なった入力インタフェースによって識別可能である。さらに、入力コンテンツが５ＣＤＴＣＰに準拠したコピー制御情報を有するか、具体的にはデジタルデータとしてのＴＳパケットに付加されたコピー制御情報を有するか、または電子透かしとして付加されたコピー制御情報を有するかを示す情報等、コンテンツに設定されたコピー制御情報の態様が判別可能な情報を含めることが好ましい。５ＣＤＴＣＰに従ったデジタルデータ入力、あるいはＢＳ，ＣＳ等の配信コンテンツには、コピー制御情報の態様がコンテンツに対する付加情報として配信する構成が実現または検討されており、記録再生装置は、このような付加情報からコピー制御情報の詳細情報の取得が可能である。

入力ソース情報を著作権情報として格納する理由について説明する。これは、入力ソースによって、そのコンテンツの取り扱いルールが異なる場合があるからであり、どんなソースからの入力かを再生処理時に取得して、再生処理における出力形態の決定、再生制限情報として用いる。たとえば、５ＣＤＴＣＰなどのコンテンツ保護方式においては、その方式で保護されたコンテンツを受信した機器は、その格納コンテンツの出力態様が規定される。

図１１に入力ソースに対応する出力制限例を示す。たとえば、入力ソースが、５ＣＤＴＣＰに従ったソースからのデータ入力である場合の記録データについての再生出力は、アナログ出力の場合には、水平ラインが５００本以下で、アナログコピー防止方式であるマクロビジョン（MacroVision）の信号を付加すれば出力が許可される。また、デジタル出力の場合には、５Ｃが認めたコンテンツ保護方式でコンテンツが保護される場合にのみ、出力が許される。その他、ＢＳ，ＣＳからの入力データを記録したデータ、地上波データ、その他各種の入力ソースからのデータに対応してそれぞれアナログ出力、デジタル出力の態様が規制される。なお、図１１に示す例は１つの規制例として示すものであり、現実の規制内容に必ずしも一致するものではない。

出力制限規定はそれぞれの保護方式によって違うので、統一的に扱おうとすると、一番制限の強いものに合わせなければならない。しかしできればよりよい画質、音質をユーザに提供したいので、再生側でディスク上に記録されたそれぞれのコンテンツのソースがわかるようにしておき、それに基づいて従うべき出力規

定を参照すれば、その中で任意の方式を選択することが可能になる。コンテンツに対応して記録媒体に格納する著作権情報中にソース情報を含めることにより、再生処理時の規制に従った再生出力が可能となる。再生出力処理については、後段で説明する。

（３）タイトル別コピー制御情報

次に、タイトル別コピー制御情報について説明する。記録媒体の格納コンテンツを、ある機器から別の機器に高速でコピーすることを考える。コンテンツは暗号化された状態で記録されている。復号、再暗号化には処理が必要となるため、暗号化された状態のまま高速コピーを行いたい。しかし、コンテンツが、「コピー禁止」の制御情報を持つ場合には、コピーは行えず、「コピーフリー」のコンテンツ（もしくは部分）についてのみ処理が可能となる。コンテンツ記録の単位であるブロック毎には、コピー制御情報（ＣＣＩ）が記されているが、これはもし改ざんされたら、コンテンツの正しい復号が行えない、という機構で保護されている。

しかし、コンテンツの復号を行なわずにコピーを実行する場合、コピー制御情報に基づく正しいコピー制御が実行されない危険性がある。すなわち、「コピー禁止」というコピー制御情報を持つブロックが含まれるコンテンツに対して、不正なユーザが、1)そのブロックのＣＣＩを「コピーフリー」に書きかえ、2)高速コピーを行い、3)コピー元とコピー先の両方のブロックのコピー制御情報を「コピー禁止」に書きかえる、という手順を踏むことによって、「コピー禁止」のコンテンツのコピーが作るという不正コピー処理が行なわれる可能性がある。

このため、復号処理を行なわないコピーであっても有効なコピー制御を行うことを可能とするためタイトル別コピー制御情報をコンテンツにリンクさせて記録する。なお、後段で説明するが、本発明の記録再生装置においては、記録媒体に対する１つの格納処理コンテンツは暗号処理キーとしてタイトルキーが対応付けられる。タイトル別コピー制御情報は、記録媒体に対する１つの格納処理コンテンツに含まれるブロックのＣＣＩから選択された最も制限の厳しい最厳格コピー制御情報である。例えば格納コンテンツのコピー制御情報として、コピーフリーと１世代コピー可が検出された場合には、タイトル別コピー制御情報として（１

世代コピー可をコピーした後の)「これ以上のコピー禁止」が記録される。こうしておけば、少なくとも最終的なコピー制御情報がコピーフリーであるコンテンツは、それに含まれるどのコピー制御情報もコピーフリーであることがわかるため、暗号を復号しなくても、高速コピーのために送信してよいということが判断でき、処理の軽減が行える。

次に、著作権情報中に含まれる記録モードについて、説明する。記録モードとは、コンテンツ記録をデータ解析記録方式（Cognizant Mode)、またはデータ非解析記録方式(Non-Cognizant Mode)のいずれのモードで実行したかを区別したデータである。

コンテンツはそれぞれあらかじめコンテンツ提供者によっていかなる条件で複製が可能かを指定されている。そこで、ネットワーク接続においてもその指定された条件を正しく相手の機器に伝える必要性があり、企業５社の共同提案としての５Ｃ ＤＴＣＰ (Digital Transmission Content Protection) システムではコピー制御情報（ＣＣＩ：Copy Control Information）という方法を用いて解決している。コピー制御情報（ＣＣＩ）はデバイスの能力に応じて２種類の伝達方法が規定されている。

エンクリプションモード･インディケータ(ＥＭＩ:Encryption Mode Indicator)はパケットヘッダにあるＳｙビットの上位２ビットを使ってコピー制御情報（ＣＣＩ）を送るメカニズムであり、受信デバイスが簡単にアクセスする事ができると同時に、この値がコンテンツを暗号化する鍵に作用するため安全に送ることができるようになっている。

ＥＭＩによりそのパケットの暗号化モードを示し、コンテンツ暗号・復号鍵の生成モードを指定する。ＥＭＩを IEEE1394 パケットヘッダに置くことにより、受信機器は例えばＭＰＥＧ転送ストリーム（MPEG transport stream）の中に埋め込まれている埋め込みコピー制御情報（Embedded CCI）（後述）を取り出すことなく簡単にどのモードでコンテンツが暗号化されているかを知ることがでる。

図１２にＩＥＥＥ１３９４パケットフォーマットを示す。データフィールド（Data Field）中には、音楽データ、画像データ等、様々なコンテンツが格納され、コピー制御情報（ＣＣＩ）としてのエンクリプション・モード・インディケ

ータ（ＥＭＩ：Encryption Mode Indicator）はパケットヘッダにあるＳｙビットの上位２ビットに設定される。

ＥＭＩの２ビット情報は、設定値に応じてコンテンツの異なる取り扱いを規定する。具体的には、値００は認証も暗号化も必要がなく、コンテンツは自由にコピーが可能なコピーフリー（Copy Free）を示し、値０１は一世代コピーの作成が可能な コピー１ジェネレーション（Copy One Generation）を、値１０は前述のCopy One Generation が一度記録された後の、再コピーが禁止されているノーモアコピー（No More Copies）を、値１１はコンテンツがリリース時点からコピー禁止であるネバーコピー（Never Copy）を表す。

Ｄ－ＶＨＳやハードディスクのような記録されるデータのフォーマットを認識しないようなビットストリームレコーダでも正しく著作物を取り扱えるように、記録時に埋め込みＣＣＩ（Embedded CCI）の更新（ｅｘ．Copy One Generation から No More Copies へ）を必要とせず、ＥＭＩの更新のみ行えばよい、という記録方法がデータ非解析（Non-Cognizant)記録方式である。

一方、こういったコピー制御情報を送るための場所があらかじめ確保されているようなフォーマット（たとえばＤＶフォーマット：DV－format）においては、ＣＣＩはコンテンツの一部として伝送することができる。このように、コンテンツの一部としてコンテンツに埋め込まれたコピー制御情報（ＣＣＩ）を埋め込みＣＣＩ（Embedded CCI）と呼ぶ。通常、コンテンツが暗号化されて転送される場合、埋め込みＣＣＩ（Embedded CCI）もコンテンツと同様に暗号化されて転送され、埋め込みＣＣＩ（Embedded CCI）の故意の変更は困難とされている。

ここで、前述したＥＭＩの２ビットのコピー制御情報と、埋め込みＣＣＩ（Embedded CCI）との双方を持つコンテンツの場合、コンテンツ記録を実行するある記録デバイスは、ＥＭＩおよび埋め込みＣＣＩ（Embedded CCI）の双方のコピー制御情報の更新を行なう。しかし、埋め込みＣＣＩ（Embedded CCI）の解析能力のない記録デバイスの場合、ＥＭＩは更新するが、埋め込みＣＣＩ（Embedded CCI）の更新は実行しないことになる。

コンテンツ記録時に、記録デバイスがコンテンツの一部として伝送された埋め込みＣＣＩ（Embedded CCI）の更新を行ってコンテンツとともに記録する記録方

式をデータ解析（Cognizant)記録方式という。データ解析（Cognizant)記録方式と、データ非解析（Non-Cognizant)記録方式では、データ非解析（Non-Cognizant)記録方式の方が埋め込みＣＣＩ（Embedded CCI）の更新を行わなくてよい分、負荷が軽く実装しやすいが、５Ｃ ＤＴＣＰのルールとして、その機器がコンテンツをＭＰＥＧデコードしてアナログ端子から映像信号を表示するためにはその機器はデータ解析記録方式（Cognizant Mode)でなければならないというルールがあり、デコード／表示機能を持つ機器はデータ解析記録方式（Cognizant Mode)を実行する機能を備えていることが必要である。

しかしまた、データ解析記録方式（Cognizant Mode)を実行するためには、コンテンツの一部として埋め込まれている埋め込みＣＣＩ（Embedded CCI）の位置や意味を完全に知る必要があり、たとえばある機器が市場に出た後に制定された新規のあるいは更新されたデータフォーマットについては、その新しいデータフォーマットに対して、古い機器がデータ解析記録方式（Cognizant Mode)を実行するのは非常に困難となる場合がある。

従って、コンテンツを記録するある機器が、特定のデータフォーマットについては、もしくは、特定の機能を実現するときには、データ解析記録方式（Cognizant Mode)を実行し、また異なるデータフォーマットのコンテンツ記録時には、データ非解析記録方式（Non-Cognizant Mode)を実行するといった、両方の記録方式を実行することが考えられる。

また、すべてのコンテンツに対して、データ非解析記録方式（Non-Cognizant Mode)の記録しか行わない機器も存在する。また、逆に埋め込みＣＣＩ（Embedded CCI）を理解できるフォーマットを持つコンテンツの処理しか実行しない機器、すなわちデータ解析記録方式（Cognizant Mode)のみ実行する機器も存在することが考えられる。

このように、２つのコピー制御情報、すなわちＥＭＩと埋め込みＣＣＩ（Embedded CCI）が存在し、またコンテンツ記録を実行する機器としても、データ解析記録方式（Cognizant Mode)を実行する機器と、データ非解析記録方式（Non-Cognizant Mode)の記録を実行する機器が混在する状況においては、データ解析記録方式（Cognizant Mode)で記録したコンテンツと、データ非解析記録方式

(Non-Cognizant Mode)で記録したコンテンツは明確に区別されることが好ましい。

すなわち、データ解析記録方式（Cognizant Mode)でコンテンツを記録した場合にはＥＭＩも埋め込みＣＣＩ（Embedded CCI）の双方のコピー制御情報が更新されるが、データ非解析記録方式（Non-Cognizant Mode)でコンテンツの記録が実行された場合は、ＥＭＩのみが更新され、埋め込みＣＣＩ（Embedded CCI）の更新が行なわれない。その結果、記録媒体上のＥＭＩと埋め込みＣＣＩ(Embedded CCI)に不整合がおこり、その両者が混ざると混乱が生じるためである。従って、２つのコピー制御情報の不整合を発生させないためには、データ解析記録方式（Cognizant Mode)で記録されたコンテンツは、データ解析記録方式（Cognizant Mode)モードでの記録再生処理を実行し、データ非解析記録方式（Non-Cognizant Mode)で記録されたコンテンツはデータ非解析記録方式（Non-Cognizant Mode)モードで記録再生処理を実行する構成とすることが必要となる。

このためには、このデータ解析記録方式（Cognizant Mode)と、データ非解析記録方式（Non-Cognizant Mode)とをまったく別の記録方式とすることも一案ではあるが、この場合、１つの機器において両方のモードを選択的に実行可能とするためには、１機器に両モードの実行処理構成を装備することが必要となり、これは、機器のコスト高を招くという問題がある。

本発明の記録再生装置では、この２つの記録方式、すなわちデータ解析記録方式（Cognizant Mode)と、データ非解析記録方式（Non-Cognizant Mode)のいずれの方式を適用するかに応じて、コンテンツ暗号処理用の鍵を異なる鍵として生成して使用する構成とすることで、機器および記録方式に応じて２つの記録方式を明確に区別して、両方式が無秩序に混在して実行される事態を解消し、機器および記録方式に応じたいずれか一方の統一的な記録方式によるコンテンツ処理構成を、機器の装備および処理負荷を増大させることなく実現している。

具体的には、データ解析記録方式（Cognizant Mode)記録用の秘密情報（再生時にも必要）としての暗号化、復号処理鍵生成用のキー（データ解析記録方式用キー（Cognizant Key））をデータ解析記録方式（Cognizant Mode)による記録または再生を行える機能を持つ機器にのみ提供して機器内に格納する構成とし、一方、

データ非解析記録方式(Non-Cognizant Mode)記録用の秘密情報(再生時にも必要)としての暗号化、復号処理鍵生成用のキー（データ非解析記録方式用キー（Non-Cognizant Key)）を、データ非解析記録方式（Non-Cognizant Mode)による記録または再生を行える機能を持つ機器にのみ提供して機器内に格納する構成とした。

著作権情報中に記録モードを格納することにより、例えば、データ解析記録方式（Cognizant Mode)で記録されたコンテンツについて、バグを原因として、あるいはデータの改竄、記録再生プログラムの不正改造等によって、データ非解析記録方式（Non-Cognizant Mode)の記録再生機能のみを有する機器において、誤ってまたは不正な記録再生の実行を防止することができる。

（４）コピー制御情報変化点

次に、著作権情報中に格納する記録コンテンツにおけるコピー制御情報の変化点を示す情報としての対応パケットナンバーと変化点におけるコピー制御情報について説明する。コンテンツ中には、一般に様々なデータが混在しており、コピー禁止の部分や、コピーフリーの部分、コピー１世代可として設定した部分が混在する。これらの検出された様々なコピー制御情報の変化点をその変化したコピー制御情報とともに著作権情報中に記録する。

変化点は、具体的には、トランスポートストリームを構成するＴＳパケットの識別子としてのパケットＮｏが使用可能である。図１３に著作権情報中に格納するコピー制御情報変化点データ例を示す。図１３に示す例は、ＴＳパケット番号［００］においてコピーフリー（００）であり、その後、ＴＳパケット番号［３００００］が変化点として抽出され、この変化点においてコピー１世代可（１０）に変化し、さらに、変化点：ＴＳパケット［１０００００］においてコピーフリー（００）に変化し、さらに、変化点：ＴＳパケット［１２３４５６７］においてコピー１世代可（１０）に変化したコンテンツであることを示している。

このようなコピー制御情報の変化点を著作権情報中に格納することにより、例えばコピーフリーの部分のみを抽出してコピー（記録媒体に格納）する処理が効率的に実行可能となり、特に高速コピー処理において有効となる。

このように、著作権情報（Copyright Information）には、コンテンツの入力ソース情報、記録機器の電子透かし世代情報（前述の第１、２，３世代)、記録モー

ドの各情報と、コンテンツ中から取得されるコピー制御情報であるＣＣＩから選択された最も厳しい最厳格コピー制御情報としてのタイトル別コピー制御情報、さらに、記録コンテンツにおけるコピー制御情報の変化点を示す情報としての対応パケットナンバーと変化点におけるコピー制御情報があり、これらの情報中から１以上の情報を著作権情報として設定し、ＭＡＣ（Message Authentication Code）を生成、付加して記録媒体に格納する。これら著作権情報の格納処理、利用処理については、後段のコンテンツの記録再生処理の説明中において、再度詳細に説明する。

［６．キー配信構成としてのツリー（木）構造について］

本発明の記録再生装置は、コンテンツの暗号化処理を行なって記録媒体に格納する処理が可能な構成を持つものであり、コンテンツ暗号処理に直接または間接的に適用する鍵を正当なライセンスを受けている記録再生装置にのみ安全に配布するためにキー配信構成としてのツリー（木）構造が用いられる。以下、このキー配信構成について説明する。

図１または図２に示した記録再生装置が、データを記録媒体に記録、もしくは記録媒体から再生する際に必要なマスターキーを、各機器に配布する構成について説明する。図１４は、本方式を用いた記録システムにおける記録再生装置の鍵の配布構成を示した図である。図１４の最下段に示すナンバ０～１５が個々の記録再生装置である。すなわち図１４に示す木（ツリー）構造の各葉(リーフ：leaf)がそれぞれの記録再生装置に相当する。

各デバイス０～１５は、製造時（出荷時）に、あらかじめ定められている初期ツリーにおける、自分のリーフからルートに至るまでのノードに割り当てられた鍵（ノードキー）および各リーフのリーフキーを自身で格納する。図１４の最下段に示すＫ０００００～Ｋ１１１１が各デバイス０～１５にそれぞれ割り当てられたリーフキーであり、最上段のＫＲから、最下段から２番目の節（ノード）に記載されたキー：ＫＲ～Ｋ１１１をノードキーとする。

図１４に示すツリー構成において、例えばデバイス０はリーフキーＫ００００と、ノードキー：Ｋ０００、Ｋ００、Ｋ０、ＫＲを所有する。デバイス５はＫ０１０１、Ｋ０１０、Ｋ０１、Ｋ０、ＫＲを所有する。デバイス１５は、Ｋ１１１

１、Ｋ１１１、Ｋ１１、Ｋ１、ＫＲを所有する。なお、図１４のツリーにはデバイスが０～１５の１６個のみ記載され、ツリー構造も４段構成の均衡のとれた左右対称構成として示しているが、さらに多くのデバイスがツリー中に構成され、また、ツリーの各部において異なる段数構成を持つことが可能である。

また、図１４のツリー構造に含まれる各記録再生器には、様々な記録媒体、例えばＤＶＤ、ＣＤ、ＭＤ、ＨＤ、メモリスティック（商標）等を使用する様々なタイプの記録再生器が含まれている。さらに、様々なアプリケーションサービスが共存することが想定される。このような異なるデバイス、異なるアプリケーションの共存構成の上に図１４に示すキー配布構成が適用されている。

これらの様々なデバイス、アプリケーションが共存するシステムにおいて、例えば図１４の点線で囲んだ部分、すなわちデバイス０，１，２，３を同一の記録媒体を用いるひとつのグループとして設定する。例えば、この点線で囲んだグループ内に含まれるデバイスに対しては、まとめて、共通のコンテンツを暗号化してプロバイダから送付したり、共通に使用するマスターキーを送付したり、あるいは各デバイスからプロバイダあるいは決済機関等にコンテンツ料金の支払データをやはり暗号化して出力するといった処理が実行される。コンテンツプロバイダ、あるいは決済処理機関等、各デバイスとのデータ送受信を行なう機関は、図１４の点線で囲んだ部分、すなわちデバイス０，１，２，３を１つのグループとして一括してデータを送付する処理を実行する。このようなグループは、図１４のツリー中に複数存在する。

なお、ノードキー、リーフキーは、ある１つの鍵管理センタによって統括して管理してもよいし、各グループに対する様々なデータ送受信を行なうプロバイダ、決済機関等によってグループごとに管理する構成としてもよい。これらのノードキー、リーフキーは例えばキーの漏洩等の場合に更新処理が実行され、この更新処理は鍵管理センタ、プロバイダ、決済機関等が実行する。

このツリー構造において、図１４から明らかなように、１つのグループに含まれる３つのデバイス０，１，２，３はノードキーとして共通のキーＫ００、Ｋ０、ＫＲを保有する。このノードキー共有構成を利用することにより、例えば共通のマスターキーをデバイス０，１，２，３のみに提供することが可能となる。たと

えば、共通に保有するノードキーＫ００自体をマスターキーとして設定すれば、新たな鍵送付を実行することなくデバイス０，１，２，３のみが共通のマスターキーの設定が可能である。また、新たなマスターキーKmasterをノードキーＫ００で暗号化した値Ｅｎｃ（Ｋ００，Kmaster）を、ネットワークを介してあるいは記録媒体に格納してデバイス０，１，２，３に配布すれば、デバイス０，１，２，３のみが、それぞれのデバイスにおいて保有する共有ノードキーＫ００を用いて暗号Ｅｎｃ（Ｋ００，Kmaster）を解いてマスターキー：Kmasterを得ることが可能となる。なお、Ｅｎｃ（Ｋａ，Ｋｂ）はＫｂをＫａによって暗号化したデータであることを示す。

また、ある時点ｔにおいて、デバイス３の所有する鍵：Ｋ００１１,Ｋ００１，Ｋ００,Ｋ０,ＫＲが攻撃者（ハッカー）により解析されて露呈したことが発覚した場合、それ以降、システム（デバイス０，１，２，３のグループ）で送受信されるデータを守るために、デバイス３をシステムから切り離す必要がある。そのためには、ノードキー：Ｋ００１,Ｋ００,Ｋ０,ＫＲをそれぞれ新たな鍵Ｋ（ｔ）００１,Ｋ（ｔ）００,Ｋ（ｔ）０,Ｋ（ｔ）Ｒに更新し、デバイス０，１，２にその更新キーを伝える必要がある。ここで、Ｋ（ｔ）ａａａは、鍵Ｋａａａの世代（Generation）：ｔの更新キーであることを示す。

更新キーの配布処理ついて説明する。キーの更新は、例えば、図１５（Ａ）に示す有効化キーブロック（ＥＫＢ：Enabling Key Block）と呼ばれるブロックデータによって構成されるテーブルをたとえばネットワーク、あるいは記録媒体に格納してデバイス０，１，２に供給することによって実行される。

図１５（Ａ）に示す有効化キーブロック（ＥＫＢ）には、ノードキーの更新の必要なデバイスのみが更新可能なデータ構成を持つブロックデータとして構成される。図１５の例は、図１４に示すツリー構造中のデバイス０，１，２において、世代ｔの更新ノードキーを配布することを目的として形成されたブロックデータである。図１４から明らかなように、デバイス０，デバイス１は、更新ノードキーとしてＫ（ｔ）００、Ｋ（ｔ）０、Ｋ（ｔ）Ｒが必要であり、デバイス２は、更新ノードキーとしてＫ（ｔ）００１、Ｋ（ｔ）００、Ｋ（ｔ）０、Ｋ（ｔ）Ｒが必要である。

図１５（Ａ）のＥＫＢに示されるようにＥＫＢには複数の暗号化キーが含まれる。最下段の暗号化キーは、Ｅｎｃ（Ｋ００１０，Ｋ（ｔ）００１）である。これはデバイス２の持つリーフキーＫ００１０によって暗号化された更新ノードキーＫ（ｔ）００１であり、デバイス２は、自身の持つリーフキーによってこの暗号化キーを復号し、Ｋ（ｔ）００１を得ることができる。また、復号により得たＫ（ｔ）００１を用いて、図１５（Ａ）の下から２段目の暗号化キーＥｎｃ（Ｋ（ｔ）００１，Ｋ（ｔ）００）を復号可能となり、更新ノードキーＫ（ｔ）００を得ることができる。以下順次、図１５（Ａ）の上から２段目の暗号化キーＥｎｃ（Ｋ（ｔ）００，Ｋ（ｔ）０）を復号し、更新ノードキーＫ（ｔ）０、図１５（Ａ）の上から１段目の暗号化キーＥｎｃ（Ｋ（ｔ）０，Ｋ（ｔ）Ｒ）を復号しＫ（ｔ）Ｒを得る。一方、デバイス０，１は、ノードキーＫ０００は更新する対象に含まれておらず、更新ノードキーとして必要なのは、Ｋ（ｔ）００、Ｋ（ｔ）０、Ｋ（ｔ）Ｒである。デバイス０，１は、図１５（Ａ）の上から３段目の暗号化キーＥｎｃ（Ｋ０００，Ｋ（ｔ）００）を復号しＫ（ｔ）００、を取得し、以下、図１５（Ａ）の上から２段目の暗号化キーＥｎｃ（Ｋ（ｔ）００，Ｋ（ｔ）０）を復号し、更新ノードキーＫ（ｔ）０、図１５（Ａ）の上から１段目の暗号化キーＥｎｃ（Ｋ（ｔ）０，Ｋ（ｔ）Ｒ）を復号しＫ（ｔ）Ｒを得る。このようにして、デバイス０，１，２は更新した鍵Ｋ（ｔ）Ｒを得ることができる。なお、図１５（Ａ）のインデックスは、復号キーとして使用するノードキー、リーフキーの絶対番地を示す。

図１４に示すツリー構造の上位段のノードキー:Ｋ０,ＫＲの更新が不要であり、ノードキーＫ００のみの更新処理が必要である場合には、図１５（Ｂ）の有効化キーブロック（ＥＫＢ：Enabling Key Block）を用いることで、更新ノードキーＫ（ｔ）００をデバイス０，１，２に配布することができる。

図１５（Ｂ）に示すＥＫＢは、例えば特定のグループにおいて共有する新たなマスターキーを配布する場合に利用可能である。具体例として、図１４に点線で示すグループ内のデバイス０，１，２，３がある記録媒体を用いており、新たな共通のマスターキーＫ（ｔ）masterが必要であるとする。このとき、デバイス０，１，２，３の共通のノードキーＫ００を更新したＫ（ｔ）００を用いて新たな共

通の更新マスターキー：K（t）master を暗号化したデータＥｎｃ（K（t），K（t）master）を図１５（Ｂ）に示すＥＫＢとともに配布する。この配布により、デバイス４など、その他のグループの機器においては復号されないデータとしての配布が可能となる。

すなわち、デバイス０，１，２はＥＫＢを処理して得たK（t）００を用いて上記暗号文を復号すれば、t時点でのマスターキーK（t）masterを得ることが可能になる。

（ＥＫＢを使用したマスターキーの配布）

図１６に、t時点でのマスターキーK（t）masterを得る処理例として、K（t）００を用いて新たな共通のマスターキーK（t）masterを暗号化したデータＥｎｃ（K（t）００，K（t）master）と図１５（Ｂ）に示すＥＫＢとを記録媒体を介して受領したデバイス０の処理を示す。

図１６に示すように、デバイス０は、記録媒体に格納されている世代：t時点のＥＫＢと自分があらかじめ格納しているノードキーＫ０００を用いて上述したと同様のＥＫＢ処理により、ノードキーK（t）００を生成する。さらに、復号した更新ノードキーK（t）００を用いて更新マスターキーK（t）masterを復号して、後にそれを使用するために自分だけが持つリーフキーＫ００００で暗号化して格納する。なお、デバイス０が更新マスターキーK（t）masterを安全に自身内に格納できる場合、リーフキーＫ００００で暗号化する必要はない。

また、この更新マスターキーの取得処理を図１７のフローチャートにより説明する。なお、記録再生装置は出荷時にその時点で最新のマスターキー:K（c）masterを与えられ、自身のメモリに安全に（具体的にはたとえば、自身のリーフキーで暗号化して）格納しているものとする。

更新マスターキーK（n）masterとＥＫＢの格納された記録媒体が、記録再生装置にセットされると、まず最初に、ステップＳ１４０１において、記録再生装置は、記録媒体から、記録媒体に格納されているマスターキーK（n）masterの時点(世代)番号:n(これを、プレ(pre－recording)記録世代情報(Generation#n)と呼ぶことにする)を読み出す。記録媒体には、予め、マスターキーK(n)masterの時点（世代）番号：nが記憶されている。また、自身が保持している暗号化マ

スターキーＣを読み出し、ステップＳ１４０２において、その暗号化マスターキーの世代：ｃと、プレ記録世代情報 Generation#n が表す世代：ｎとを比較して、その世代の前後を判定する。

ステップＳ１４０２において、プレ記録世代情報 Generation#n が表す世代：ｎの方が、自身のメモリに記憶された暗号化マスターキーＣの世代：ｃよりも後でない（新しくない）と判定された場合、即ち、メモリに記憶された暗号化マスターキーＣの世代：ｃが、プレ記録世代情報 Generation#n が表す世代：ｎと同一か、または後の場合、ステップＳ１４０３乃至Ｓ１４０８をスキップして、マスターキー更新処理を終了する。即ち、この場合、自身のメモリに記憶されたマスターキーＫ（ｃ）master（暗号化マスターキーＣ）の更新は行う必要がないので、その更新は行われない。

一方、ステップＳ１４０２において、プレ記録世代情報 Generation#n が表す世代：ｎの方が、メモリに記憶された暗号化マスターキーＣの世代：ｃよりも後である（新しい）と判定された場合、即ち、メモリに記憶された暗号化マスターキーＣの世代が、プレ記録世代情報 Generation#n が表す世代ｎよりも前の世代である場合、ステップＳ１４０３に進み、記録再生装置は、記録媒体から、有効化キーブロック（ＥＫＢ：Enabling Key Block)を読み出す。

ステップＳ１４０４において、記録再生装置は、ステップＳ１４０３で読み出したＥＫＢと、自身がメモリに格納しているリーフキー（図１４のデバイス０におけるＫ００００）およびノードキー（図１４のデバイス０におけるＫ０００，Ｋ００...）を用いて、プレ記録世代情報 Generation#n（図１６におけるｔ）時点でのノード００の鍵Ｋ（ｔ）００を計算する。

ステップＳ１４０５では、ステップＳ１４０４においてＫ（ｔ）００を得られたか否かを検査する。得られなかった場合は、その時点においてその記録再生装置がツリー構成のグループからリボーク（排除）されていることを示すので、ステップＳ１４０６乃至Ｓ１４０８をスキップしてマスターキー更新処理を終了する。

Ｋ（ｔ）００を得られた場合、ステップＳ１４０６に進み、記録媒体からＥｎｃ（Ｋ（ｔ）００，Ｋ（ｔ）master)、すなわち、Ｋ（ｔ）００を用いてｔ時点で

のマスターキーを暗号化した値を読み出す。そしてステップＳ１４０７において、この暗号文をＫ（ｔ）００を用いて復号してＫ（ｔ）masterを計算する。

ステップＳ１４０８では、自身のみが持つリーフキー（図１４のデバイス０におけるＫ００００）を用いてＫ（ｔ）masterを暗号化してメモリに格納する。以上で、マスターキーの更新処理が完了する。

ところで、マスターキーは、時点（世代）０から昇順に使用されていくが、新しい世代のマスターキーから、古い世代のマスターキーを計算によりシステム内の各機器が求められる構成とすることが望ましい。すなわち、記録再生装置は、一方向性関数ｆを保持しており、その一方向性関数ｆに、自身が持つマスターキーを、そのマスターキーの世代と、必要なマスターキーの世代との差に対応する回数だけ適用することにより、調べた世代のマスターキーを作成する。

具体的には、例えば、記録再生装置に記憶されているマスターキーＭＫの世代が世代ｉ＋１であり、あるデータの再生に必要な（記録時に使用された）マスターキーＭＫの世代が世代ｉ－１である場合、マスターキーＫ（ｉ－１）masterは、記録再生装置において、一方向性関数ｆが２回用いられ、ｆ（ｆ（Ｋ（ｉ＋１）master））を計算することにより生成される。

また、記録再生装置に記憶されているマスターキーの世代が世代ｉ＋１であり、必要なマスターキーの世代が世代ｉ－２である場合、マスターキーＫ（ｉ－２）masterは、一方向性関数ｆを３回用いて、ｆ（ｆ（ｆ（Ｋ（ｉ＋１）master）））を計算することにより生成される。

ここで、一方向性関数としては、例えば、ハッシュ(hash)関数を用いることができる。具体的には、例えば、ＭＤ５(Message Digest 5)や、ＳＨＡ－１(Secure Hash Algorithm - 1)等を採用することができる。キーを発行するキー発行機関は、これらの一方向性関数を用いて自身の世代より前の世代を生成可能なマスターキーＫ（０）master，Ｋ（１）master，Ｋ（２）master・・・，Ｋ（Ｎ）masterを、あらかじめ求めておく。即ち、まず最初に、第Ｎ世代のマスターキーＫ(Ｎ)masterを設定し、そのマスターキーＫ（Ｎ）masterに、一方向性関数を１回ずつ適用していくことで、それより前の世代のマスターキーＫ（Ｎ－１）master，Ｋ（Ｎ－２）master，・・・，Ｋ（１）master，Ｋ（０）masterを順次生成しておく。そし

て、世代の小さい（前の）マスターキーＫ（０）masterから順番に使用していく。なお、自身の世代より前の世代のマスターキーを生成するのに用いる一方向性関数は、すべての記録再生装置に設定されているものとする。

また、一方向性関数としては、例えば、公開鍵暗号技術を採用することも可能である。この場合、キー発行機関は、公開鍵暗号方式の秘密鍵を所有し、その秘密鍵に対する公開鍵を、すべての再生装置に与えておく。そして、キー発行機関は、第０世代のマスターキーＫ（０）masterを設定し、そのマスターキーＫ（０）masterから使用していく。即ち、キー発行機関は、第１世代以降のマスターキーＫ(ｉ)masterが必要になったら、その１世代前のマスターキーＫ(ｉ－１)masterを、秘密鍵で変換することにより生成して使用する。この場合、キー発行機関は、一方向性関数を用いて、Ｎ世代のマスターキーを、あらかじめ生成しておく必要がない。また、この方法によれば、理論上は、無制限の世代のマスターキーを生成することができる。なお、記録再生装置では、ある世代のマスターキーを有していれば、そのマスターキーを、公開鍵で変換することにより、その世代より前の世代のマスターキーを得ることができる。

［７．マスターキーを用いた暗号処理によるコンテンツの記録再生］

次に、マスターキーを用いた暗号処理によるコンテンツの記録再生処理について説明する。まず、記録再生装置がコンテンツを自身の記録媒体に記録する場合に実行されるマスターキーの判別処理について図１８のフローチャートを用いて説明する。コンテンツデータは、ある世代のマスターキーにより暗号化されてネットワークあるいは記録媒体を介してコンテンツプロバイタから各記録再生装置に配布される。

まず最初に、ステップＳ１５０１において、記録再生装置は、記録媒体から、プレ記録世代情報Generation#nを読み出す。また、自身のメモリが記憶している暗号化マスターキーＣの世代ｃを取得し、ステップＳ１５０２において、その暗号化マスターキーの世代ｃと、プレ記録世代情報Generation#nが表す世代ｎとを比較して、その世代の前後を判定する。

ステップＳ１５０２において、メモリに記憶された暗号化マスターキーＣの世代ｃが、プレ記録世代情報Generation#nが表す世代ｎ以後でないと判定された場

合、即ち、メモリに記憶された暗号化マスターキーＣの世代ｃが、プレ記録世代情報 Generation#n が表す世代ｎよりも古い世代である場合、ステップＳ１５０３をスキップして、すなわち、コンテンツデータの記録処理を行わずに終了する。

一方、ステップＳ１５０２において、自身の記録再生装置内のメモリに記憶された暗号化マスターキーＣの世代が、プレ記録世代情報 Generation#n が表す世代ｎ以後であると判定された場合、即ち、メモリに記憶された暗号化マスターキーＣの世代が、プレ記録世代情報 Generation#n が表す世代ｎと同一か、またはそれよりも新しい場合、ステップＳ１５０３に進み、コンテンツデータの記録処理を行う。

コンテンツデータの記録処理に際しては、前述したように、記録装置自体の該当する電子透かし処理態様に従った電子透かし検出処理、埋め込み処理が実行される。これは、上述した第１世代、第２世代、第３世代の各世代に従って、第１世代であれば電子透かしの検出、埋め込み双方の処理の非実行、第２世代であれば検出のみ、第３世代であれば検出、および埋め込みを実行する。さらに、コンテンツに対応して生成する著作権情報内に記録装置の電子透かし世代情報を格納する。

これらの電子透かしに対する処理に並列して、コンテンツの格納のための暗号化処理が実行される。以下、マスターキーを用いたコンテンツ暗号化処理の詳細について説明する。なお、マスターキーは上述したように世代管理のなされたキーである。ここでは、先に説明したトランスポートストリームによって構成されるデータを世代管理されたマスターキーを利用してブロックキーを生成してブロックキーによりコンテンツデータを暗号化して記録媒体に格納する処理について説明する。

図１９、図２０のブロック図を用いて説明する。図１９、図２０は、暗号処理手段１５０における処理を説明するため、各データ、処理をブロック化して示した図である。なお、ここでは、記録媒体として光ディスクを例とする。この実施例では、記録媒体上のデータの bit-by-bit コピーを防ぐために、記録媒体固有の識別情報としてのディスクＩＤ(Disc ID)を、データを暗号化する鍵に作用させるようにしている。

記録再生装置１６００は自身のメモリ１８０（図１，２参照）に格納しているマスターキー１６０１、データ解析記録方式用キー(コグニザントキー:Cognizant Key) １６３１もしくはデータ非解析記録方式用キー（ノンコグニザントキー：Non-Cognizant Key) １６３２を読み出す。

マスターキー１６０１は、先に説明した図１７のフローに従って記録再生装置のメモリに格納された秘密キーであり、前述のように世代管理がなされており、それぞれに世代番号が対応付けられている。このマスターキーは、複数の記録再生装置に共通なキー、例えば図１４に示す点線枠のグループに属するデバイスに共通なキーである。デバイスＩＤは記録再生装置１６００の識別子であり、予め記録再生装置に格納されている例えば製造番号等の識別子である。このデバイスＩＤは公開されていてもよい。データ解析記録方式用キー（Cognizant Key）１６３１、データ非解析記録方式用キー（Non-Cognizant Key）１６３２は、それぞれの記録モードに対応したキーであり、複数の記録再生装置に共通のキーである。これらは予め記録再生装置１６００のメモリに格納されている。

記録再生装置１６００は例えば光ディスクである記録媒体１６２０に識別情報としてのディスクＩＤ（Disc ID）１６０３が既に記録されているかどうかを検査する。記録されていれば、ディスクＩＤ（Disc ID）１６０３を読出し（図１９に相当)、記録されていなければ、暗号処理手段１５０においてランダムに、もしくはあらかじめ定められた例えば乱数発生等の方法でディスクＩＤ（Disc ID）１７０１を生成し、ディスクに記録する（図２０に相当)。ディスクＩＤ（Disc ID）１６０３はそのディスクにひとつあればよいので、リードインエリアなどに格納することも可能である。

記録再生装置１６００は、次にマスターキーと、特殊な読み取り方法でのみディスクから読み取り可能な秘密情報として記録されたスタンパーＩＤ（Stamper ID）１６８０と、ディスクＩＤ１６０３を用いて、ディスク固有キー(Disc Unique Key）を生成１６０２する。

マスターキーと秘密情報としてのスタンパーＩＤ（Stamper ID）１６８０とディスクＩＤ１６０３とを用いディスク固有キー（Disc Unique Key）の具体的な生成方法を図２１を用いて説明する。図２１に示すように、ブロック暗号関数を用

いたハッシュ関数にマスターキー（Master Key）とスタンパーＩＤ（Stamper ID）とディスクＩＤ（Disc ID）を入力して得られた結果を用いる例１の方法や、FIPS 180-1 で定められているハッシュ関数ＳＨＡ－１に、マスターキーとスタンパーＩＤ(Stamper ID)とディスクＩＤ（Disc ID）とのビット連結により生成されるデータを入力し、その１６０ビットの出力から必要なデータ長のみをディスク固有キー（Disc Unique Key）として使用する例２の方法が適用できる。

上述したように、スタンパーＩＤ（Stamper ID）１６８０は、あらかじめディスクに記録されている高度な秘密情報であり、その読出しおよび読み出されたスタンパーＩＤ（Stamper ID）を利用したディスク固有キー（Disc Unique Key）の生成などの演算処理は、秘密が保たれるように暗号処理手段内部で実行される。すなわち、ディスクから読み出された秘密情報は暗号処理手段内においてセキュアに保護される。

このように、本発明の構成においては、正当なデバイスのみが、たとえばＬＳＩ内に実装されて高度に保護された暗号鍵の生成を実行する暗号処理部においてセキュアな保護の下にコンテンツ暗号処理用の鍵生成処理を実行する構成であり、不正なコンテンツの再生処理を効果的に防止することが可能となる。

記録再生装置１６００は、次に、記録コンテンツごとの固有鍵であるタイトルキー（Title Key）１６０４を暗号処理手段１５０（図１，２，参照）においてランダムに、もしくはあらかじめ定められた例えば乱数発生等の方法で生成１６０４し、ディスク１６２０に記録する。

記録再生装置１６００は、さらに、使用するマスターキーの世代番号、すなわち、自身が格納するマスターキーの世代番号［記録時世代番号（Generation#n)］１６５０を取得して、これを記録媒体１６２０に記録時世代番号１６５１として格納する。

ディスク上には、どこのデータがどんなタイトルを構成するかという情報が格納されたデータ管理ファイルがあり、このファイルにタイトルキー１６０５、記録モードフラグ１６３５、マスターキーの世代番号［記録時世代番号(Generation#n)］１６５１を格納することができる。

なお、記録媒体１６２０には、予め、プレ（pre－recording）世代番号が格納

されており、プレ世代番号と同一またはプレ世代番号より新しい世代のマスターキーを用いて暗号化されて格納されたコンテンツのみの再生を可能とする構成となっている。この構成については、後段の再生処理の欄で説明する。

次にディスク固有キー（Disc Unique Key）とタイトルキー（Title Key）と、データ解析記録方式用キー（Cognizant Key)、あるいは、ディスク固有キー（Disc Unique Key）とタイトルキー（Title Key）と、データ非解析記録方式用キー（Non-Cognizant Key)、いずれかの組合せから、タイトル固有キー（Title Unique Key）を生成する。

すなわち、記録モードがデータ解析記録方式（Cognizant Mode)である場合には、ディスク固有キー（Disc Unique Key）とタイトルキー（Title Key）と、データ解析記録方式用キー(Cognizant Key)とからタイトル固有キー(Title Unique Key)を生成し、記録モードがデータ非解析記録方式（Non-Cognizant Mode)である場合には、ディスク固有キー（Disc Unique Key）とタイトルキー（Title Key）と、データ非解析記録方式用キー（Non-Cognizant Key)とからタイトル固有キー（Title Unique Key）を生成する。

前述したように、データ解析記録方式（Cognizant Mode)記録用の秘密情報としての暗号化、復号処理鍵生成用のキー（データ解析記録方式用キー（Cognizant Key）は、データ解析記録方式（Cognizant Mode)による記録または再生を行える機能を持つ機器のみが有し、一方、データ非解析記録方式（Non-Cognizant Mode）記録用の秘密情報としての暗号化、復号処理鍵生成用のキー（データ非解析記録方式用キー(Non-Cognizant Key)は、データ非解析記録方式(Non-Cognizant Mode)による記録または再生を行える機能を持つ機器のみが有する。従って、一方の記録方式にのみ対応した機器においては、いずれか一方のモードのみを選択してコンテンツ記録が実行される。すなわち、データ解析記録方式用キー（Cognizant Key)を用いるか、あるいはデータ非解析記録方式用キー（Non-Cognizant Key)を用いるかの一方のみに限られることとなる。

しかし、両者のキーを格納し、両モードの記録方式を実行可能な機器においては、いずれのモードによる記録を実行するかを決定する処理が必要となる。このモード決定プロセス処理について、すなわち、コンテンツの記録をデータ解析記

録方式（Cognizant Mode)によって実行するか、データ非解析記録方式（Non-Cognizant Mode)で実行するかを決定するプロセスについて図２２を用いて説明する。

基本的には、コンテンツ記録は、できる限りデータ解析記録方式（Cognizant Mode)によって実行するのが望ましい。これは、前述したように、ＥＭＩと埋め込みＣＣＩ（Embedded CCI）との不整合を生じさせないためである。ただし、前述したように、新規なデータフォーマットの出現等によるデータ解析エラー等の発生の可能性もあり、このような場合に、データ非解析記録方式（Non-Cognizant Mode)での記録処理を実行する。

図２２の各ステップについて説明する。ステップＳ５００１では、記録装置は、データ・フォーマットを解析可能か否かを判定する。先に説明したように、埋め込みＣＣＩ（Embedded CCI）は、コンテンツの内部に埋め込まれており、データフォーマットの解析が不可能であれば、埋め込みＣＣＩ（Embedded CCI）の読み取りが不可能となるので、この場合は、データ非解析記録方式（Non-Cognizant Mode)での記録処理を実行する。

データフォーマットの解析が可能であれば、ステップＳ５００２に進み、記録装置が、データ（コンテンツ）のデコード処理、埋め込みＣＣＩ（Embedded CCI）の読み取り、更新処理が可能か否かを判定する。コンテンツおよび埋め込みＣＣＩ（Embedded CCI)は通常、符号化（エンコード）されており、埋め込みＣＣＩ（Embedded CCI)の読み取りには復号（デコード）を実行することが必要となる。例えば多チャンネル同時記録などの際に、復号回路が他に使用されているなど理由で、機器が復号処理可能でない場合は、埋め込みＣＣＩ（Embedded CCI)の読み取りができないので、データ非解析記録方式（Non-Cognizant Mode)での記録処理を実行する。

ステップＳ５００２のデータ（コンテンツ）のデコード処理、埋め込みＣＣＩ（Embedded CCI)の読み取り、更新処理が可能であると判定されると、ステップＳ５００３において、記録装置に対するユーザ入力中に、データ非解析モードでの記録処理の実行指定入力があるか、否かが判定される。この処理は、ユーザの指定によるモード選択を可能とした機器においてのみ実行されるステップであり、

通常の機器、すなわちユーザによるモード指定を許容しない機器においては実行されない。ユーザ入力によるデータ非解析記録方式（Non-Cognizant Mode)での記録処理指定があった場合は、データ非解析記録方式（Non-Cognizant Mode)での記録処理が実行される。

次に、ステップＳ５００４において、コンテンツパケット（ｅｘ．受信データ）中に、データ非解析モードでの記録処理の実行指定があるか否かが判定される。データ中にデータ非解析モードでの記録処理の実行指定がある場合は、データ非解析記録方式（Non-Cognizant Mode)での記録処理が実行される。指定がない場合は、データ解析記録方式（Cognizant Mode)での記録処理が実行される。

データ解析記録方式（Cognizant Mode)での記録処理、およびデータ非解析記録方式（Non-Cognizant Mode)での記録処理の双方を選択的に実行可能な機器においては、上述したモード決定プロセス処理によって、いずれのモードでの記録を実行するかが決定される。ただし、図２１の処理フローからも理解されるように、データ解析記録方式（Cognizant Mode)での記録が可能な場合は、基本的にデータ解析記録方式（Cognizant Mode)での処理が実行されることになる。

前述したように、記録モードをデータ解析記録方式（Cognizant Mode)とした場合は、ディスク固有キー（Disc Unique Key）とタイトルキー（Title Key）と、データ解析記録方式用キー（Cognizant Key)からタイトル固有キー（Title Unique Key）を生成し、記録モードをデータ非解析記録方式（Non-Cognizant Mode)とした場合は、ディスク固有キー（Disc Unique Key）とタイトルキー（Title Key）と、データ非解析記録方式用キー（Non-Cognizant Key)とからタイトル固有キー（Title Unique Key）を生成する。

タイトル固有キー（Title Unique Key）生成の具体的な方法を図２３に示す。図２３に示すように、ブロック暗号関数を用いたハッシュ関数にタイトルキー（Title Key）とディスク固有キー（Disc Unique Key）と、データ解析記録方式用キー（Cognizant Key）（データ解析記録方式（Cognizant Mode)の場合）、もしくは、データ非解析記録方式用キー（Non-Cognizant Key）（データ非解析記録方式（Non-Cognizant Mode)の場合）を入力して得られた結果を用いる例１の方法、あるいは、FIPS 180-1で定められているハッシュ関数ＳＨＡ－１に、マスターキ

ーとディスクＩＤ（Disc ID）とデータ解析記録方式用キー（Cognizant Key）（データ解析記録方式（Cognizant Mode)の場合）もしくはデータ非解析記録方式用キー（Non-Cognizant Key）（データ非解析記録方式（Non-Cognizant Mode)の場合）とのビット連結により生成されるデータを入力し、その１６０ビットの出力から必要なデータ長のみをタイトル固有キー（Title Unique Key）として使用する例２の方法が適用できる。

なお、上記の説明では、マスターキー（Master Key）とスタンパーＩＤ(Stamper ID)とディスクＩＤ（Disc ID）からディスク固有キー（Disc Unique Key）を生成し、これとタイトルキー(Title Key)とデータ解析記録方式用キー(Cognizant Key)もしくはデータ非解析記録方式用キー（Non-Cognizant Key)からタイトル固有キー（Title Unique Key）をそれぞれ生成するようにしているが、ディスク固有キー（Disc Unique Key）を不要としてマスターキー（Master Key）とディスクＩＤ（Disc ID)とタイトルキー(Title Key)と、データ解析記録方式用キー(Cognizant Key)もしくはデータ非解析記録方式用キー（Non-Cognizant Key)から直接タイトル固有キー（Title Unique Key）を生成してもよく、また、タイトルキー（Title Key）を用いずに、マスターキー（Master Key）とディスクＩＤ（Disc ID）と、データ解析記録方式用キー（Cognizant Key)もしくはデータ非解析記録方式用キー（Non-Cognizant Key)からタイトル固有キー（Title Unique Key）相当の鍵を生成してもよい。

たとえば上記の５ＣＤＴＣＰに規定される伝送フォーマットのひとつを使用した場合、データはＭＰＥＧ２のＴＳパケットで伝送される場合がある。たとえば、衛星放送を受信したセットトップボックス（ＳＴＢ：Set Top Box）がこの放送を記録機に５ＣＤＴＣＰを用いて伝送する際に、ＳＴＢは衛星放送通信路で伝送されたＭＰＥＧ２　ＴＳパケットをＩＥＥＥ１３９４上も伝送することが、データ変換の必要がなく望ましい。

記録再生装置１６００は記録すべきコンテンツデータをこのＴＳパケットの形で受信し、前述したＴＳ処理手段３００において、各ＴＳパケットを受信した時刻情報であるＡＴＳを付加する。なお、先に説明したように、ブロックデータに付加されるブロック・シードは、ＡＴＳとコピー制御情報、さらに他の情報を組

み合わせた値から構成してもよい。

ＡＴＳを付加したＴＳパケットをＸ個（例えばＸ＝３２）並べて、１ブロックのブロックデータが形成（図５の上の図参照）され、図１９、図２０の下段に示すように、被暗号化データとして入力されるブロックデータの先頭の第 1～４バイトが分離され（セレクタ１６０８）て出力される３２ビットのＡＴＳを含むブロックシード(Block Seed)と、先に生成したタイトル固有キー(Title Unique Key)とから、そのブロックのデータを暗号化する鍵であるブロック・キー(Block Key)が生成１６０７される。

ブロック・キー（Block Key）の生成方法の例を図２４に示す。図２４では、いずれも３２ビットのブロック・シード（Block Seed）と、６４ビットのタイトル固有キー（Title Unique Key）とから、６４ビットのブロックキー（Block Key）を生成する例を２つ示している。

上段に示す例１は、鍵長６４ビット、入出力がそれぞれ６４ビットの暗号関数を使用している。タイトル固有キー（Title Unique Key）をこの暗号関数の鍵とし、ブロックシード（Block Seed）と３２ビットの定数（コンスタント）を連結した値を入力して暗号化した結果をブロックキー（Block Key）としている。

例２は、FIPS 180-1 のハッシュ関数ＳＨＡ－１を用いた例である。タイトル固有キー（Title Unique Key）とブロックシード（Block Seed）を連結した値をＳＨＡ－１に入力し、その１６０ビットの出力を、たとえば下位６４ビットのみ使用するなど、６４ビットに縮約したものをブロックキー（Block Key）としている。

なお、上記ではディスク固有キー(Disc Unique key)、タイトル固有キー(Title Unique Key)、ブロックキー（Block Key）をそれぞれ生成する例を説明したが、たとえば、ディスク固有キー(Disc Unique Key)とタイトル固有キー(Title Unique Key）の生成を実行することなく、ブロックごとにマスターキー（Master Key）とスタンパーＩＤ(Stamper ID)とディスクＩＤ（Disc ID）とタイトルキー（Title Key）とブロックシード（Block Seed）と、データ解析記録方式用キー（Cognizant Key）（Cognizant Mode の場合）もしくはデータ非解析記録方式用キー（Non-Cognizant Key）（データ非解析記録方式（Non-Cognizant Mode)の場合）を用いてブロックキー（Block Key）を生成してもよい。

ブロックキーが生成されると、生成されたブロックキー（Block Key）を用いてブロックデータを暗号化する。図１９、図２０の下段に示すように、ブロックシード（Block Seed）を含むブロックデータの先頭の第 1～mバイト（たとえばｍ＝８）は分離（セレクタ１６０８）されて暗号化対象とせず、ｍ＋１バイト目から最終データまでを暗号化１６０９する。なお、暗号化されないmバイト中にはブッロク・シードとしての第 1～４バイトも含まれる。セレクタ１６０８により分離された第ｍ＋１バイト以降のブロックデータは、暗号処理手段１５０に予め設定された暗号化アルゴリズムに従って暗号化１６０９される。暗号化アルゴリズムとしては、たとえば FIPS 46-2 で規定されるＤＥＳ（Data Encryption Standard）を用いることができる。

また、前述したようにブロック・シードには、コピー制限情報(ＣＣＩ：Copy Control Information)を含ませることが可能であり、データ解析記録方式（Cognizant Mode)での記録処理を実行した場合には、コンテンツデータ内部に埋め込まれたコピー制御情報（ＣＣＩ）である埋め込みＣＣＩ（Embedded CCI）に対応するコピー制御情報が記録され、また、データ非解析記録方式(Non-Cognizant Mode)での記録処理を実行した場合には、図２０で説明したパケットヘッダ上のＥＭＩ（Encyrption Mode Indicator)を反映したコピー制御情報が記録される。

すなわち、データ解析記録方式（Cognizant Mode)による情報記録処理の場合、データ部内の埋め込みコピー制御情報（ＣＣＩ）に基づくコピー制御情報を含むブロックシードを、1 以上のパケットからなるブロックデータに付加した記録情報生成処理を実行し、データ非解析記録方式（Non-Cognizant Mode)による情報記録処理の場合、パケットに含まれるコピー制御情報としてのエンクリプション・モード・インディケータ（ＥＭＩ）に基づくコピー制御情報を含むブロックシードを、1 以上のパケットからなるブロックデータに付加した記録情報生成処理を実行する。

ここで、使用する暗号アルゴリズムのブロック長（入出力データサイズ）がＤＥＳのように８バイトであるときは、Ｘを例えば３２とし、ｍを例えば８の倍数とすることで、端数なくｍ＋１バイト目以降のブロックデータ全体が暗号化できる。

すなわち、１ブロックに格納するＴＳパケットの個数をＸ個とし、暗号アルゴリズムの入出力データサイズをＬバイトとし、ｎを任意の自然数とした場合、１９２＊Ｘ＝ｍ＋ｎ＊Ｌが成り立つようにＸ，ｍ、Ｌを定めることにより、端数処理が不要となる。

暗号化した第ｍ＋１バイト以降のブロックデータは暗号処理のされていない第1～ｍバイトデータとともにセレクタ１６１０により結合されて暗号化コンテンツ１６１２として記録媒体１６２０に格納される。

さらに、本発明の記録再生装置においては、記録処理に係るコンテンツに対応する著作権情報（Copyright Information）を生成し、さらに、その改竄チェック値としてのＭＡＣ（Message Authentication Code）を生成１６５１して、ディスク１６２０に著作権情報＆ＭＡＣ１６５２を記録する。

前述したように、著作権情報（Copyright Information）は、例えば、入力ソース情報、記録機器の電子透かし世代情報（前述の第１、２，３世代)、記録モードの各情報、コンテンツ中から取得されるコピー制御情報としてのＣＣＩから選択された最も厳しい最厳格コピー制御情報であるタイトル別コピー制御情報、さらに、記録コンテンツにおけるコピー制御情報の変化点を示す情報としての対応パケットナンバーと変化点におけるコピー制御情報などであり、これらの情報中から１以上の情報を著作権情報として設定して記録媒体に格納する

様々な著作権情報の生成処理例を図２５、図２６、図２７を参照して説明する。図２５は、著作権情報として、入力ソース情報、記録機器電子透かし世代情報、記録モードを格納する例である。記録モード（Recording Mode）は、実行する情報記録モードが、データ解析記録方式（Cognizant Mode)であるか、データ非解析記録方式（Non-Cognizant Mode)であるかを示す。

図２５のステップＳ５１０１では、入力ソースを判定し、８ビットの入力ソース情報を生成格納する。入力ソース情報は、５ＣＤＴＣＰに準拠した入力ソースからのコンテンツであるか、ＢＳ，ＣＳ等の衛星配信コンテンツであるか、地上波デジタルコンテンツであるか、地上波アナログコンテンツであるかなどの入力ソース情報である。入力ソース情報の構成例を以下に示す。

入力ソース：

0x00：IEEE1394 with 5C

0x01：IEEE1394 without 5C

0x02：USB with 5C

0x03：USB without 5C

0x04：内蔵 BS Tuner

0x05：内蔵 CS Tuner

0x06：内蔵地上波 Tuner

0x07：アナログ

0x08-ff：リザーブ

ステップＳ５１０２では、自装置のＲＯＭに格納された記録機器の電子透かし世代情報（８ビット）を取得してする。記録機器の電子透かし世代情報は、前述したように、電子透かしの処理態様で区分した第１～第３世代の機器を示すものであり、コンテンツの記録を実行する自己装置の情報を示す。電子透かし世代情報の構成例を以下に示す。

記録機器電子透かし世代情報：

0x00：第１世代

0x01：第２世代

0x02：第３世代

0x03-ff：リザーブ

ステップＳ５１０３では、コンテンツの記録モードを取得する。記録モードは、データ解析記録方式（Cognizant Mode)かデータ非解析記録方式（Non-cognizant)かを示す１ビット情報である。記録モードの情報構成例を以下に示す。

記録モード：

0：データ解析記録方式（Cognizant Mode)

1：データ非解析記録方式（Non-cognizant)

ステップＳ５１０４では、著作権情報を６４ビット構成とするために残りビットとして４７ビットのリザーブデータ”０”を格納する。この処理によって、６４ビットの著作権情報が生成される。

図２６は、著作権情報として、記録対象コンテンツ中の各ブロックデータから

取得されるＣＣＩから最も厳しい最厳格コピー制御情報を選択してこれをタイトル別コピー制御情報として格納し、さらに、記録モードを格納する例である。記録モード（Recording Mode）は、実行する情報記録モードが、データ解析記録方式（Cognizant Mode)であるか、データ非解析記録方式（Non-Cognizant Mode)であるかを示す。

図２６のステップＳ５２０１では、記録動作中、各ブロックデータに付与されたコピー制御情報（ＣＣＩ）を検証し、最も厳しい最厳格コピー制御情報を選択する。厳しいコピー制御情報は、コピー禁止、１世代コピー可、これ以上コピー禁止、コピーフリーの順である。選択したコピー制御情報を８ビットのタイトル別コピー制御情報とする。タイトル別コピー制御情報の構成例を以下に示す。

タイトル別コピー制御情報：

0x00：コピーフリー

0x01：これ以上コピー禁止

0x02：１世代コピー可

0x03：コピー禁止

0x04-ff：リザーブ

ステップＳ５２０２では、コンテンツの記録モードを取得する。記録モードは、データ解析記録方式（Cognizant Mode)かデータ非解析記録方式（Non-cognizant）かを示す情報である。

ステップＳ５２０３では、著作権情報を６４ビット構成とするために残りビットとして５５ビットのリザーブデータ”０”を格納する。この処理によって、６４ビットの著作権情報が生成される。

図２７は、著作権情報として、記録モードおよびコピー制御情報の変化点情報を格納する例である。

ステップＳ５３０１では、、コンテンツの記録モードを取得する。記録モードは、データ解析記録方式（Cognizant Mode)かデータ非解析記録方式（Non-cognizant）かを示す情報である。

次に、ステップＳ５３０２では、記録対象コンテンツ中の各ブロックデータから取得されるＣＣＩの変化点を取得し、変化点の位置情報を示すパケットＮｏ．

と変化点におけるコピー制御情報のデータを取得する。これは、例えば先に図１３を用いて説明したデータであり、変化点を示すバケットＮｏを３０ビット、対応するコピー制御情報を２ビットとしたデータである。

さらに、ステップＳ５３０３では、著作権情報を６４ビットまたは６４ビットの倍数構成とするために残りビットのパディング処理として調整ビットに”０”を格納する。この処理によって、６４ビットの倍数の著作権情報が生成される。

このように、著作権情報として格納されるデータ構成は様々な態様が可能である。上述した例では説明していないが、入力ソース情報、記録機器の電子透かし世代情報（前述の第１、２，３世代)、記録モードの各情報、コンテンツ中から取得されるコピー制御情報としてのＣＣＩから選択された最も厳しい最厳格コピー制御情報であるタイトル別コピー制御情報、さらに、記録コンテンツにおけるコピー制御情報の変化点を示す情報としての対応パケットナンバーと変化点におけるコピー制御情報のすべてを著作権情報として格納してもよい。

上述した様々な著作権情報に対して改竄検証値データとしてのＭＡＣが生成されて、著作権情報はＭＡＣとともに記録媒体に格納される。ＭＡＣ生成処理例を図２８を用いて説明する。図２８に示すように、６４ビットブロック暗号関数を用いたハッシュ関数にディスク固有キーとタイトルキーと、上述した著作権情報を入力して算出した結果をＭＡｃとする例１の方法や、FIPS 180-1で定められているハッシュ関数ＳＨＡ－１に、ディスク固有キーとタイトルキーと著作権情報とのビット連結により生成されるデータを入力し、その１６０ビットの出力から必要なデータ長のみを著作権情報ＭＡＣ値として使用する例２の方法が適用可能である。

以上の処理により、コンテンツはブロック単位で、世代管理されたマスターキー、ＡＴＳを含むブロック・シード等に基づいて生成されるブロック鍵で暗号化が施されて記録媒体に格納されるとともに、コンテンツに対応する著作権情報が改竄チェック用のＭＡＣと共に格納される。

上述のように、本構成では、世代管理されたマスターキーによりコンテンツデータが暗号化され記録媒体に格納されているので、その記録媒体を他の記録再生器における再生処理は、少なくとも同一世代、あるいはデータを記録した際に使

用されたマスターキーの世代より新しい世代を有する記録再生器であることが復号、すなわち再生可能となる条件となる。

さらに、コンテンツに対応して記録媒体に著作権情報が格納され、再生、出力時に記録媒体に格納された暗号化コンテンツの復号を行なうことなく著作権情報を取得することが可能となり、再生制御、出力制御が正しく実行される。また、記録媒体を他の再生装置に設定して再生する場合においても、著作権情報中にソース情報、あるいは電子透かし世代情報を参照することにより、コンテンツ記録機器において設定されたコピー制御情報を正しく判定することが可能となるので、正しい再生制御が実行される。なお、コンテンツ再生処理の詳細については、後段で説明する。

次に図２９に示すフローチャートに従って、データ記録処理にともなって実行されるＴＳ処理手段３００におけるＡＴＳ、ＣＣＩ付加処理および暗号処理手段１５０における暗号処理の処理全体の流れをまとめて説明する。なお、電子透かし検出、埋め込み処理手段１８５における処理は、記録機器の電子透かし世代に従った処理が、図２９に示す処理フローに並列して実行されるものとする。すなわち、機器が第１世代であれば、電子透かしの検出、埋め込みとも実行されず、第２世代であれば検出のみ実行し、第３世代であれば、検出、埋め込みの双方の処理が実行されるものとする。図２９の処理フローは、これら電子透かし処理と並列して実行されるＴＳ処理手段３００におけるＡＴＳ、ＣＣＩ付加処理および暗号処理手段１５０における暗号処理の処理を説明するフローである。

図２９のＳ１８０１において、記録再生装置は自身のメモリ１８０に格納しているマスターキーおよび データ解析記録方式用キー（Cognizant Key）（データ解析記録方式（Cognizant Mode)の場合）もしくはデータ非解析記録方式用キー（Non-Cognizant Key）（データ非解析記録方式（Non-Cognizant Mode)の場合）を読み出す。また、ディスクからスタンパーＩＤ(Stamper ID)を読み出す。

Ｓ１８０２において、記録媒体に識別情報としてのディスクＩＤ（Disc ID）が既に記録されているかどうかを検査する。記録されていればＳ１８０３でこのディスクＩＤを読出し、記録されていなければＳ１８０４で、ランダムに、もしくはあらかじめ定められた方法でディスクＩＤを生成し、ディスクに記録する。次

に、Ｓ１８０５では、マスタキーと スタンパーＩＤ(Stamper ID)とディスクＩＤを用いて、ディスク固有キーを生成する。ディスク固有キーは先に図２１を用いて説明したように、例えば、FIPS 180-1 で定められているハッシュ関数ＳＨＡ－１を用いる方法やブロック暗号に基づくハッシュ関数を使用する方法などを適用することで求める。

次にＳ１８０６に進み、その一回の記録ごとの固有の鍵としてのタイトルキー(Title Key) を生成し、マスターキーの世代番号とともにディスクに記録する。

次にＳ１８０７で、上記のディスク固有キーとタイトルキーと、データ解析記録方式用キー (Cognizant Key) (データ解析記録方式 (Cognizant Mode)の場合) もしくはデータ非解析記録方式用キー (Non-Cognizant Key) (データ非解析記録方式 (Non-Cognizant Mode)の場合) から、タイトル固有キーを生成する。

タイトル固有キーの生成の詳細フローを図３０に示す。暗号処理手段１５０は、ステップＳ２００１において、記録モードにより分岐する。この分岐は、記録再生器のプログラムや、記録再生器を使用するユーザによって入力された指示データに基づいて判定される。

Ｓ２００１で記録モードがデータ解析記録方式 (Cognizant Mode)、すなわち、Cognizant 記録の場合は、ステップＳ２００２に進み、ディスク固有キー (Disc Unique Key)とタイトルキー(Title Key)と、データ解析記録方式用キー(Cognizant Key)とから、タイトル固有キー (Title Unique Key) を生成する。

Ｓ２００１で記録モードがデータ非解析記録方式 (Non-Cognizant Mode)、すなわち、Non-Cognizant 記録の場合は、ステップＳ２００３に進みディスク固有キー (Disc Unique Key) とタイトルキー (Title Key) と、データ非解析記録方式用キー (Non-Cognizant Key)とから、タイトル固有キー (Title Unique Key) を生成する。キー生成には、ＳＨＡ－１を用いる方法やブロック暗号に基づくハッシュ関数を使用する。

Ｓ１８０８では、記録再生装置は記録すべきコンテンツデータの被暗号化データをＴＳパケットの形で受信する。Ｓ１８０９で、ＴＳ処理手段３００は、各ＴＳパケットを受信した時刻情報であるＡＴＳを付加する。あるいはコピー制御情報ＣＣＩとＡＴＳ、さらに他の情報を組み合わせた値を付加する。次に、Ｓ１８

１０で、ＡＴＳを付加したＴＳパケットを順次受信し、１ブロックを形成する例えばＸ＝３２に達したか、あるいはパケットの終了を示す識別データを受信したかを判定する。いずれかの条件が満足された場合はステップＳ１８１１に進み、Ｘ個、あるいはパケット終了までのパケットを並べて、１ブロックのブロックデータを形成する。

次に、暗号処理手段１５０は、Ｓ１８１２で、ブロックデータの先頭の３２ビット（ＡＴＳを含むブロック・シード）とＳ１８０７で生成したタイトル固有キーとから、そのブロックのデータを暗号化する鍵であるブロックキーを生成する。

Ｓ１８１３では、ブロックキーを用いてＳ１８１１で形成したブロックデータを暗号化する。なお、先にも説明したように、暗号化の対象となるのは、ブロックデータのｍ＋１バイト目から最終データまでである。暗号化アルゴリズムは、たとえばFIPS 46-2で規定されるＤＥＳ（Data Encryption Standard）が適用される。

Ｓ１８１４で、暗号化したブロックデータを記録媒体に記録する。Ｓ１８１５で、全データを記録したかを判断する。全データを記録していれば、記録処理を終了し、全データを記録していなければＳ１８０８に戻って残りのデータの処理を実行する。

さらに、ステップＳ１８１６、Ｓ１８１７において、この記録処理に係るコンテンツに対応する著作権情報（Copyright Information）を生成し、さらに、その改竄チェック値としてのＭＡＣ（Message Authentication Code）を生成して、ディスクに著作権情報＆ＭＡＣを記録する。前述したように、著作権情報(Copyright Information)は、例えば、入力ソース情報、記録機器の電子透かし世代情報（前述の第１、２，３世代)、記録モードの各情報、コンテンツ中から取得されるコピー制御情報としてのＣＣＩから選択された最も厳しい最厳格コピー制御情報であるタイトル別コピー制御情報、さらに、記録コンテンツにおけるコピー制御情報の変化点を示す情報としての対応パケットナンバーと変化点におけるコピー制御情報などであり、これらの情報中から１以上の情報を著作権情報として設定して記録媒体に格納する。著作権情報の生成処理例は、先に、図２５、図２６、図２７を参照して説明した通りであり、ＭＡＣ生成処理は、図２８を用いて説明した

処理にしたがって実行される。

上述の処理にしたがって、コンテンツに対応して記録媒体に著作権情報が格納され、再生、出力時に記録媒体に格納された暗号化コンテンツの復号を行なうことなく著作権情報を取得することが可能となり、再生制御、出力制御が正しく実行される。また、記録媒体を他の再生装置に設定して再生する場合においても、著作権情報に格納されたソース情報、あるいは電子透かし世代情報を参照することにより、コンテンツ記録機器において設定されたコピー制御情報を正しく判定することが可能となるので、正しい再生制御が実行される。

次に、上記のようにして記録媒体に記録された暗号化コンテンツを復号して再生する処理について図３１の処理ブロック図と、図３２のフローを用いて説明する。

図３２に示すフローチャートに従って、復号処理および再生処理について、処理の流れを説明する。図３２のＳ２４０１において、記録再生装置２３００（図３１参照）はディスク２３２０からディスクＩＤ２３０２とプレ（pre－recording）記録世代番号とスタンパーＩＤ(Stamper ID)２３８０を読み出し、また自身のメモリからマスターキー２３０１、データ解析記録方式用キー（Cognizant Key)２３３１および／あるいはデータ非解析記録方式用キー（Non-Cognizant Key)２３３２を読み出す。先の記録処理の説明から明らかなように、ディスクＩＤはディスクにあらかじめ記録されているか、そうでない場合は記録再生器において生成してディスクに記録したディスク固有の識別子である。

プレ（pre－recording）記録世代番号２３６０は、予め記録媒体であるディスクに格納されたディスク固有の世代情報である。このプレ（pre－recording）世代番号と、データ記録時のマスターキーの世代番号、すなわち記録時世代番号２３５０を比較して再生処理の可否を制御する。マスターキー２３０１は、図１７のフローにより記録再生装置のメモリに格納され世代管理のなされた秘密キーである。データ解析記録方式用キー（Cognizant Key)およびデータ非解析記録方式用キー（Non-Cognizant Key)は、それぞれデータ解析（Cognizant）記録モードおよびデータ非解析（Non-Cognizant）記録モードに対応したシステム共通の秘密キーである。

記録再生装置２３００は、次に、Ｓ２４０２で、ディスクから読み出すべきデータのタイトルキー、改竄チェックデータとしてのＭＡＣの付加された著作権情報、さらに、データを記録したときに使用したマスターキーの世代番号（Generation #）すなわち記録時世代番号２３５０を読み出す。著作権情報（Copyright Information）には、コンテンツの入力ソース情報、記録機器の電子透かし世代情報（前述の第１、２，３世代)、記録モードの各情報と、コンテンツ中から取得されるコピー制御情報であるＣＣＩから選択された最も厳しい最厳格コピー制御情報としてのタイトル別コピー制御情報、さらに、記録コンテンツにおけるコピー制御情報の変化点を示す情報としての対応パケットナンバーと変化点におけるコピー制御情報中から１以上の情報が含まれる。また、著作権情報（Copyright Information）は、容易に改ざんされないように、正当性検査コードとしてのＭＡＣ（Message Authentication Code）が付加されて記録媒体に格納されている。

ステップＳ２４０３では、ディスクＩＤ(Disc ID)とマスターキー(Master Key)とスタンパーＩＤ(Stamper ID)を用いてディスク固有キー（Disc Unique Key）を生成２３０２する。このキー生成方法は、先に図２１を用いて説明した通りであり、例えば、FIPS 180-1で定められているハッシュ関数SHA-1に、マスターキーとディスクＩＤ（Disc ID）とのビット連結により生成されるデータを入力し、その１６０ビットの出力から必要なデータ長のみをディスク固有キー(Disc Unique Key)として使用する方法や、ブロック暗号関数を用いたハッシュ関数にマスターキー（Master Key）とディスクＩＤ（Disc ID）を入力して得られた結果を用いるなどの方法が挙げられる。ここで使用するマスターキーは、図２７のステップＳ２４０２で記録媒体から読み出した、そのデータの記録時世代番号が表す世代(時点）のマスターキーである。もし記録再生装置がこれよりも新しい世代のマスターキーを保持している場合には、それを用いてディスク固有キー（Disc Unique Key）を生成してもよい。

次に、ステップＳ２４０４において、著作権情報のＭＡＣの計算を実行する。ＭＡＣ計算は、先に図２８を用いて説明した処理によって実行され、図２８に示すように、６４ビットブロック暗号関数を用いたハッシュ関数にディスク固有キ

ーとタイトルキーと著作権情報を入力して得られた結果を用いる例１の方法や、FIPS 180-1で定められているハッシュ関数ＳＨＡ－１に、ディスク固有キーとタイトルキーと著作権情報とのビット連結により生成されるデータを入力し、その１６０ビットの出力から必要なデータ長のみを著作権情報ＭＡＣ値として使用する例２の方法が適用できる。

著作権情報とともに記録媒体に格納されたＭＡＣ値と、読み出した著作権情報に基づいて新たに生成したＭＡＣ値とが等しいと判断されれば、著作権情報の改竄はないものと判断される。

ステップＳ２４０５では、このＭＡＣ判定を含む判定結果に基づいて再生可能性の判定が実行される。判定処理の詳細フローを図３３に示す。

図３３のステップＳ２５０１において、記録再生装置は、Ｓ２４０１で読み出したプレ世代番号と、Ｓ２４０２で読み出した記録時世代番号の新旧を判定する。記録時世代番号が示す世代が、プレ記録世代情報が表す世代以後でないと判定された場合、即ち、データ記録時世代情報が表す世代が、プレ記録世代情報が表す世代よりも古い世代である場合、再生不可能と判断し、図３２のステップＳ２４０６以下をスキップして、再生処理を行わずに処理を終了する。従って、記録媒体に記録されたコンテンツが、プレ記録世代情報が表す世代よりも古い世代のマスターキーに基づいて暗号化されたものである場合には、その再生は許可されず、再生は行われない。

即ち、この処理は、不正が発覚して、最新の世代のマスターキーが与えられなくなった不正な記録装置で、古い世代のマスターキーに基づいて、データが暗号化され、記録媒体に記録された場合に該当するものと判断し、そのような不正な装置によってデータが記録された記録媒体の再生は行わないとした処理である。これにより、不正な記録装置の使用を排除することができる。

一方、図３３のステップＳ２５０１において、記録時世代番号が表す世代が、プレ記録世代番号が表す世代以後であると判定された場合、即ち、記録時世代情報が表す世代が、プレ記録世代番号が表す世代ｎと同一か、または新しい世代であり、従って、記録媒体に記録されたコンテンツが、プレ記録世代情報が表す世代以後の世代のマスターキーに基づいて暗号化されたものである場合には、ステ

ップＳ２５０２に進み、記録再生装置は、自身のメモリが記憶している暗号化マスターキーＣの世代情報を取得し、その暗号化マスターキーの世代と、暗号時世代情報が表す世代を比較して、その世代の前後を判定する。

ステップＳ２５０２において、メモリに記憶されたマスターキーＣの世代が、記録時世代情報が表す世代以後でないと判定された場合、即ち、メモリに記憶されたマスターキーＣの世代が、記録時世代情報が表す世代よりも古い世代である場合、再生不可能と判断し、図３２のステップＳ２４０６以下をスキップして、再生処理を行わずに処理を終了する。

一方、ステップＳ２５０２において、メモリに記憶された暗号化マスターキーＣの世代が、記録時世代情報が表す世代以後であると判定された場合、即ち、メモリに記憶されたマスターキーＣの世代が、記録時世代情報が表す世代と同一か、またはそれよりも新しい場合、ステップＳ２５０３に進み、記録時のモードに対応する鍵、すなわちデータ解析記録方式用キー（Cognizant Key)もしくはデータ非解析記録方式用キー（Non-Cognizant Key)を、再生機器自身が所有しているかどうかを判断する。

ステップＳ２５０３において、記録時のモードに対応する鍵であるデータ解析記録方式用キー（Cognizant Key)もしくはデータ非解析記録方式用キー（Non-Cognizant Key)を、再生機器自身が所有している場合、再生可能と判定する。記録時のモードに対応する鍵（データ解析記録方式用キー（Cognizant Key)もしくはデータ非解析記録方式用キー（Non-Cognizant Key)）を、再生機器自身が所有していない場合、再生不可能と判定する。

ステップＳ２５０３において、記録時のモードに対応する鍵（データ解析記録方式用キー（Cognizant Key)もしくはデータ非解析記録方式用キー（Non-Cognizant Key)）を、再生機器自身が所有していると判定された場合は、ステップＳ２５０４に進み、図３２のステップＳ２４０４で計算したＭＡＣが正しいか否か、すなわち、記録媒体に格納されたＭＡＣと計算値としてのＭＡＣが等しいか否かが判定される。等しい場合は、ステップＳ２５０５に進み、不一致の場合は、著作権情報に改竄ありと判定されて再生不可能の処理となる。

ステップＳ２５０５では、記録媒体から読み出した著作権情報の検討が実行さ

れ、著作権情報に基づいて再生の可否が判定される。

著作権情報には、前述したように様々な態様の情報格納形態があり、その情報形態によって再生可能性の判定処理も異なることになる。図３４に著作権情報中の入力ソース情報に基づいて再生可否を判定する場合の処理フロー、図３５に著作権情報中の電子透かし世代情報に基づいて再生可否を判定する場合の処理フロー、図３６に著作権情報中のタイトル別コピー制御情報に基づいて再生可否を判定する場合の処理フローをそれぞれ示す。著作権情報に基づく再生可否は、著作権情報中に含まれる情報に従って、図３４,図３５、図３６のフローを１以上選択して実行することになる。

まず、図３４のフローについて説明する。図３４は、入力ソース情報に基づいて再生可否を判定する場合であり、まず、ステップＳ５５０１でユーザにより出力形態の指定があったか否かが判定される。出力形態とは、例えばデジタル出力としてのＩＥＥＥ１３９４Ｉ／Ｆを介した出力であり、５ＣＤＴＣＰに準拠した出力、またはＵＳＢＩ／Ｆを介したデジタル出力、あるいはアナログＩ／Ｆを介したアナログ出力などである。

ユーザが出力形態を指定している場合は、ステップＳ５５０２に進み、記録媒体から再生しようとしているコンテンツに対応した著作権情報中の入力ソース情報を参照し、予め記録再生装置内のメモリに格納している出力制限情報との対応により出力の可否を判定する。記録再生装置内のメモリに格納している出力制限情報は先に図１１を用いて説明した入力ソースに関する出力制限情報と同様のものである。

例えばユーザが指定した出力が５ＣＤＴＣＰに準拠した出力であり、再生(出力)予定コンテンツの著作権情報に格納された入力ソース情報が５ＣＤＴＣＰのデータであれば、図１１の表に示す最上段のラインのデータに相当し、出力が許可される。また、例えばユーザが指定した出力がデジタル出力であり、再生(出力)コンテンツの著作権情報に格納された入力ソース情報がＢＳであった場合は、図１１に示すルールでは出力が許可されていないので再生は行われない。ステップＳ５５０３ではこのような著作権情報に格納した入力ソースに基づく出力可否の判定がなされる。

一方、ステップＳ５５０１で、ユーザが出力形態の指定を実行していなかった場合には、ステップＳ５５０４、Ｓ５５０５において、入力ソース情報に基づく出力可能形態の有無が記録再生装置内のメモリに格納している出力制限情報（図１１に示す情報に相当する）に基づいて判定される。出力可能な形態があれば、ステップＳ５５０５でＹｅｓの判定となり、再生可能となり、出力可能な形態がない場合には、再生不可能と判定される。

次に、図３５のフローについて説明する。図３５は、電子透かし世代情報に基づいて再生可否を判定する場合である。電子透かし世代情報は、再生しようとするコンテンツを記録した記録装置の電子透かし世代（第１，第２，第３世代）であり、コンテンツ記録時にコンテンツに対応する著作権情報中に格納されたものである。

なお、本判定は、コンテンツ中から電子透かしを検出する装置において有効であり、電子透かし世代としては前述したいわゆる第２世代、第３世代の記録再生装置においてのみ実行される。また電子透かしが暗号化コンテンツではなく、復号コンテンツに対して検出、埋め込みがなされる場合は、図３５に示す判定処理は、図３２の処理フローのステップＳ２４０９のブロックデータ復号処理の後ステップにおいて実行されることになる。暗号処理データに対して電子透かしの埋め込みがなされている場合は、図３２のＳ２４０５の再生可能判定ステップにおいて実行される。

図３５のフローについて説明する。まず、ステップＳ５６０１において、検出された電子透かし情報がコピー禁止を示すか、１世代コピー可、それ以外（コピーフリーまたは、これ以上コピー禁止）であるかを判定する。コピー禁止を示している場合には、再生出力は禁止されることになる。コピーフリーまたは、これ以上コピー禁止を示している場合は、再生可と判定する。１世代コピー可である電子透かしの検出がなされた場合には、ステップＳ５６０２に進み、著作権情報中の記録機器の電子透かし世代情報を読み取り、コンテンツを記録した記録機器の電子透かし世代情報が第２世代以下である場合には、再生可と判定し、第３世代以上である場合は、再生不可と判定する。

コンテンツが第２世代の機器において記録されたコンテンツである場合は、電

子透かしの更新が実行されないことから、ユーザ書き込み可能な記録媒体にコピーされたコンテンツにコピー１世代可を示すプライマリマーク（１０）がそのままの形で電子透かしとして残存する。記録装置が第３世代であれば、コピー１世代可を示すプライマリマーク（１０）のコンテンツをコピーした場合はこれ以上コピー禁止を示す（１０１）に更新されていることになる。

再生を実行しようとする装置が、コンテンツ記録装置の電子透かし世代情報を著作権情報から取得することにより、記録装置の処理が把握でき、例えば記録装置が第２世代の機器であることが著作権情報中の電子透かし世代情報に基づいて判定された場合は、再生を実行するとするものである。この処理により、異なる世代の機器において記録、再生が実行される場合でも、電子透かし時様補に基づく正確なコピー制御が実行されることになる。

次に、図３６のフローについて説明する。図３６は、タイトル別コピー制御情報に基づいて再生可否を判定する場合である。タイトル別コピー制御情報は、コンテンツ中から取得されるコピー制御情報としてのＣＣＩから選択された最も厳しい最厳格コピー制御情報に対応した情報である。

ステップＳ５７０１において、再生を実行しようとするコンテンツに対応する著作権情報中のタイトル別コピー制御情報を取得して、タイトル別コピー制御情報がコピー禁止を示す場合は、再生不可と判定し、それ以外の場合は、再生可と判定する。

図３４、図３５、図３６の処理フローは、著作権情報中に格納された１つの情報に基づく判定処理フローを個別的に記載してあるが、例えば複数の情報が、再生予定のコンテンツに対応して記録媒体に格納された著作権情報に含まれる場合は、複数の情報に基づく判定処理をシーケンシャルにあるいはパラレルに実行して、すべての判定において再生可と判定された場合においてのみ最終的に再生可と判定し、いずれかの判定において、１つでも再生不可の判定がなされた場合には、再生不可とする処理を行なう構成とする。

これらの判定の結果に基づいて、図３３の再生可能性の判定処理が終了し、すべての条件が満足し、再生可能と判定されれば、図３２に示すステップＳ２４０６に移行する。なお、前述したように電子透かしの判定処理が復号データに対す

る電子透かし検出に基づいて実行される場合は、電子透かしに基づく再生可能性の判定は、図３２のステップＳ２４０９のブロックデータの復号処理の後に実行する。

図３２のフローに戻り、再生処理について説明を続ける。ステップＳ２４０６では、タイトル固有キーの生成を行なう。タイトル固有キーの生成の詳細フローを図３７に示す。暗号処理手段１５０は、ステップＳ２６０１において、記録モードの判定を実行する。この判定は、ディスクから読み出した著作権情報に格納された記録モード（Recording Mode）に基づいて実行される。

Ｓ２６０１において、記録モードがデータ解析記録方式（Cognizant Mode)であると判定された場合は、ステップＳ２６０２に進み、ディスク固有キー（Disc Unique Key)とタイトルキー(Title Key)と、データ解析記録方式用キー(Cognizant Key)とから、タイトル固有キー（Title Unique Key）を生成する。

Ｓ２６０１において、記録モードがデータ非解析記録方式（Non-Cognizant Mode)であると判定された場合は、ステップＳ２６０３に進み、ディスク固有キー（Disc Unique Key）とタイトルキー（Title Key）と、データ非解析記録方式用キー（Non-Cognizant Key)とから、タイトル固有キー（Title Unique Key）を生成する。キー生成には、ＳＨＡ－１を用いる方法やブロック暗号に基づくハッシュ関数を使用する。

なお、上記の説明では、マスターキー(Master Key)と スタンパーＩＤ(Stamper ID)とディスクＩＤ（Disc ID）からディスク固有キー（Disc Unique Key）を生成し、これとタイトルキー（Title Key）と データ解析記録方式用キー（Cognizant Key)もしくはデータ非解析記録方式用キー（Non-Cognizant Key)からタイトル固有キー（Title Unique Key）をそれぞれ生成するようにしているが、ディスク固有キー（Disc Unique Key）を不要としてマスターキー（Master Key）と スタンパーＩＤ(Stamper ID)とディスクＩＤ（Disc ID）とタイトルキー（Title Key）と、データ解析記録方式用キー（Cognizant Key)もしくはデータ非解析記録方式用キー（Non-Cognizant Key)から直接タイトル固有キー（Title Unique Key）を生成してもよく、また、タイトルキー（Title Key）を用いずに、マスターキー（Master Key）とスタンパーＩＤ(Stamper ID)とディスクＩＤ（Disc ID）と、デ

一タ解析記録方式用キー（Cognizant Key)もしくはデータ非解析記録方式用キー（Non-Cognizant Key)からタイトル固有キー（Title Unique Key）相当の鍵を生成してもよい。

次にＳ２４０７でディスクから暗号化されて格納されている暗号化コンテンツ２３１２から順次ブロックデータ（Block Data）を読み出し、Ｓ２４０８で、ブロックデータの先頭の４バイトのブロック・シード（Block Seed）をセレクタ２３１０において分離して、ブロックシード（Block Seed）と、Ｓ２４０６で生成したタイトル固有キーを用いてブロックキーを生成する。

ブロック・キー（Block Key）の生成方法は、先に説明した図２４の構成を適用することができる。すなわち、３２ビットのブロック・シード（Block Seed）と、６４ビットのタイトル固有キー（Title Unique Key）とから、６４ビットのブロックキー（Block Key）を生成する構成が適用できる。

なお、上記説明ではディスク固有キー（Disc Unique key)、タイトル固有キー（Title Unique Key)、ブロックキー（Block Key）をそれぞれ生成する例を説明したが、たとえば、ディスク固有キー(Disc Unique Key)とタイトル固有キー(Title Unique Key）の生成を実行することなく、ブロックごとにマスターキー（Master Key）と スタンパーＩＤ(Stamper ID)とディスクＩＤ（Disc ID）とタイトルキー（Title Key）と、ブロックシード（Block Seed）と、データ解析記録方式用キー（Cognizant Key)もしくはデータ非解析記録方式用キー（Non-Cognizant Key)を用いてブロックキー（Block Key）を生成してもよい。

ブロックキーが生成されると、次にＳ２４０９で、ブロックキー（Block Key）を用いて暗号化されているブロックデータを復号２３０９し、セレクタ２３０８を介して復号データとして出力する。なお、復号データには、トランスポートストリームを構成する各トランスポートパケットにＡＴＳが付加されており、先に説明したＴＳ処理手段３００において、ＡＴＳに基づくストリーム処理が実行される。その後、データは、使用、たとえば、画像を表示したり、音楽を再生したりすることが可能となる。

このように、ブロック単位で暗号化され記録媒体に格納された暗号化コンテンツはブロック単位でＡＴＳを含むブロック・シードに基づいて生成されるブロッ

ク鍵で復号処理が施されて再生が可能となる。ブロックキーを用いて暗号化されているブロックデータを復号し、Ｓ２４１０で、全データを読み出したかを判断し、全データを読み出していれば終了し、そうでなければＳ２４０７に戻り残りのデータを読み出す。

なお、上述した記録再生装置は、図３１に示すように、データ解析記録方式（Cognizant Mode)記録用の暗号化、復号処理鍵生成用のキー（データ解析記録方式用キー（Cognizant Key））と、データ非解析記録方式（Non-Cognizant Mode）記録用の暗号化、復号処理鍵生成用のキー（データ非解析記録方式用キー（Non-Cognizant Key））との双方を選択的に使用可能な構成例であるが、いずれか一方のキー、すなわちデータ解析記録方式用キー（Cognizant Key)、あるいはデータ非解析記録方式用キー（Non-Cognizant Key）のみを格納した機器においては、いずれか一方のみの格納キーに対応する方式のみを実行し、格納キーに基づいてコンテンツの復号処理用のブロックキーを生成する。

上述したように、本発明の情報処理装置としての再生装置は、コンテンツの再生に際し、コンテンツに対応して生成格納された著作権情報に基づいて再生、出力の可否を判定する。著作権情報には、入力ソース情報、記録機器の電子透かし世代情報（前述の第１、２，３世代)、記録モードの各情報、コンテンツ中から取得されるコピー制御情報としてのＣＣＩから選択された最も厳しい最厳格コピー制御情報であるタイトル別コピー制御情報、さらに、記録コンテンツにおけるコピー制御情報の変化点を示す情報としての対応パケットナンバーと変化点におけるコピー制御情報などであり、これらの情報中から１以上の情報を取得して再生の可否を判定する。

また、著作権情報に含まれるタイトル別コピー制御情報を用いることにより、コンテンツのコピー処理を効率的に実行することが可能となる。上述した再生処理においては、ブロックデータの復号を行なって出力していたが、例えばコンテンツ全体がコピーフリーである場合には、各ブロックに付加されたコピー制御情報（ＣＣＩ）や、電子透かしを検出することなく他の機器にコンテンツを移動（コピー）しても何ら問題はない。

再生対象コンテンツ全体がコピーフリーであるか否かを、コンテンツに対応し

て格納された著作権情報中のタイトル別コピー制御情報に基づいて判定することができる。前述したようにタイトル別コピー制御情報は、コンテンツ中から取得されるコピー制御情報としてのＣＣＩから選択された最も厳しい最厳格コピー制御情報である。従って、タイトル別コピー制御情報がコピーフリーである場合には、対応コンテンツ中のすべてがコピーフリーであることになる。従って、コンテンツ中のブロックデータに付加されたＣＣＩを確認することなく、他の機器へのコンテンツコピーが可能であると判定できることになる。

タイトル別コピー制御情報を適用したコンテンツ再生出力処理フローを図３８に示す。図３８のステップＳ６１０１では、再生対象コンテンツに対応付けられた著作権情報からタイトル別コピー制御情報を取得し、取得したタイトル別コピー制御情報がコピーフリーであるか否かを判定する。コピーフリーであれば、ステップＳ６１０２に進み、コンテンツ全体の再生出力を実行する。この場合、ブロックデータ毎のＣＣＩ判定は不要となる。従って、復号処理も省略可能である。一方、タイトル別コピー制御情報がコピーフリーでない場合には、ステップＳ６１０３に進み、コピーの許可された部分を抽出して出力することになる。この場合は、各ＣＣＩまたは電子透かし情報検出など、所定の処理を実行することが必要となる。

さらに、コンテンツに様々なコピー制御情報が含まれる場合にも、高速コピー処理を可能とするために、著作権情報に含まれる記録コンテンツにおけるコピー制御情報の変化点情報が適用される。コピー制御情報の変化点情報は、先に、図１３を用いて説明したように、コピー制御情報が変化するＴＳパケットのナンバーと、変化点におけるコピー制御情報を対応付けたデータである。

コピー制御情報の変化点情報を適用したコンテンツ再生出力処理フローを図３９に示す。図３９のステップＳ６２０１では、再生対象コンテンツに対応付けられた著作権情報からコピー制御情報変化点情報を取得し、取得したコピー制御情報変化点情報に基づいて、コンテンツ中のコピーフリー部分などコピーの許可されたコンテンツ領域を抽出する。具体的にはパケットＮｏ．に基づいて、コンテンツのコピー可能部分を特定する。

ステップＳ６２０２では、ステップＳ６２０１で抽出したコピー可能部分を選

択出力する。この場合、抽出部分はコピーが可能であることが明らかであるのでブロックデータ毎のＣＣＩ判定は不要となる。従って、復号処理も省略可能である。ただし、必要に応じてＣＣＩまたは電子透かし情報の更新処理は実行してもよい。

このように、コンテンツに対応付けた著作権情報中に格納したタイトル別コピー制御情報、コピー制御情報の変化点情報を取得して、コンテンツのコピー制御態様を判定することが可能となり、コンテンツ再生出力処理の効率化が実現される。

［８．メディアキーを用いた暗号処理によるコンテンツの記録再生］

上記の実施例は、有効化キーブロック（ＥＫＢ：Enabling Key Block）を用いて各記録再生装置に対してマスターキーを伝送し、これを用いて記録再生装置がデータの記録、再生を行うと構成例であった。

マスターキーは、その時点におけるデータの記録全体に有効な鍵であり、ある時点のマスターキーを得ることができた記録再生装置は、その時点およびそれ以前にこのシステムで記録されたデータを復号することが可能になる。ただし、システム全体で有効であるというその性質上、マスターキーが攻撃者に露呈した場合の影響がシステム全体に及ぶという不具合もある。

これに対し、記録媒体のＥＫＢ（Enabling Key Block）を用いて伝送する鍵を、全システムに有効なマスターキーではなく、その記録媒体にのみ有効なメディアキーとすることにより、キーの露呈の影響を抑えることが可能となる。以下に、第２の実施例としてマスターキーの代わりにメディアキーを用いる方式を説明する。ただし、第１の実施例との変更部分のみを説明する。

図４０には、図１６と同様の例として、デバイス０が記録媒体に格納されている ｔ 時点のＥＫＢと自分があらかじめ格納しているリーフキーＫ０００００とノードキーＫ０００，Ｋ００を用いて更新ノードキーＫ（ｔ）００を生成し、それを用いて更新メディアキー：Ｋ（ｔ）media を得る様子を示している。ここで得たＫ（ｔ）mediaは、その記録媒体のデータの記録、再生時に使用される。

なお、図４０におけるプレ記録世代番号（Generation #n)は、メディアキーにおいてはマスターキーのように世代の新旧という概念はないので必須ではなくオ

プションとして設定される。

各記録再生装置は、たとえば、データの記録もしくは再生のために記録媒体が記録再生装置に挿入された際に、図４１に示すフローチャートによってその記録媒体用のメディアキー：Ｋ（ｔ）media を計算し、後にその記録媒体へのアクセスに使用する。

図４１のステップＳ２８０１のＥＫＢの読みこみとＳ２８０２のＥＫＢの処理は、それぞれ図１７のステップＳ１４０３およびＳ１４０４と同様の処理である。

ステップＳ２８０３において記録再生装置はメディアキーＫ（ｔ）media をノードキー Ｋ（ｔ）００で暗号化した暗号文Ｅｎｃ（Ｋ（ｔ）００，Ｋ（ｔ）media）を記録媒体から読みこみ、ステップＳ２８０４でこれを復号してメディアキーを得る。もしこの記録再生装置が図１４に示すツリー構成のグループから排除、すなわちリボークされていれば、メディアキーを入手できず、その記録媒体への記録および再生が行えない。

次に、メディアキーを適用してキーを生成して、生成したキーによる暗号処理を行なって記録媒体へデータを記録する処理について説明するが、メディアキーにおいてはマスターキーのように世代の新旧という概念はないので、第１の実施例において図１８を用いて説明したプレ記録世代情報と記録再生装置自身が格納するマスターキーの世代の比較による記録可能かどうかのチェックは行わず、上記処理においてメディアキーを得られていれば記録を行えると判断する。すなわち、図４２に示す処理フローのようになる。図４２の処理フローは、メディアキーの取得をＳ２９０１で判定し、取得された場合にのみ、ステップＳ２９０２においてコンテンツの記録処理を実行するものである。

メディアキーを用いた暗号処理によるコンテンツデータの記録処理について、図４３、４４のブロック図および図４５のフローチャートを用いて説明する。

本実施例では、第１の実施例と同様、記録媒体として光ディスクを例とする。この実施例では、記録媒体上のデータの bit-by-bit コピーを防ぐために、記録媒体固有の識別情報としてのディスクＩＤ(Disc ID)を、データを暗号化する鍵に作用させるようにしている点も同様である。

図４３および図４４は、それぞれ第１の実施例における図１９および図２０に

対応する図であり、マスターキー（Master Key）の代わりにメディアキー（Media Key）が使われている点が異なっており、また、マスターキーの世代を示す記録時世代番号（Generation #）を用いていない点が異なっている。図４３および図４４の差異は、図１９、図２０の差異と同様ディスクＩＤの書き込みを実行するかしないかの差異である。

図４５はメディアキーを用いる本実施例におけるデータ記録処理を示すものであり、前述した図２９（実施例１）のフローチャートに対応する。以下、図４５の処理フローについて実施例１と異なる点を中心として説明する。

図４５のＳ３２０１において、記録再生装置３０００は自身のメモリに格納している データ解析記録方式用キー（Cognizant Key)および／もしくはデータ非解析記録方式用キー（Non-Cognizant Key)と、図４１のＳ２８０４で計算し、一時的に保存しているメディアキーＫ（ｔ）media を読み出す。また、ディスクからスタンパーＩＤ(Stamper ID)を読み出す。

Ｓ３２０２において、記録再生装置は記録媒体（光ディスク）３０２０に識別情報としてのディスクＩＤ（Disc ID）が既に記録されているかどうかを検査する。記録されていれば、Ｓ３２０３でこのディスクＩＤ（Disc ID）を読出し（図４３に相当)、記録されていなければ、Ｓ３２０４で、ランダムに、もしくはあらかじめ定められた方法でディスクＩＤ（Disc ID）を生成し、ディスクに記録する（図４４に相当)。ディスクＩＤ（Disc ID）はそのディスクにひとつあればよいので、リードインエリアなどに格納することも可能である。いずれの場合でも、次にＳ３２０５に進む。

Ｓ３２０５では、Ｓ３２０１で読み出したメディアキーとスタンパーＩＤ(Stamper ID)とディスクＩＤ(Disc ID)を用いて、ディスク固有キー(Disc Unique Key）を生成する。ディスク固有キー（Disc Unique Key）の具体的な生成方法としては、第１の実施例で使用した方法と同じ方法で、マスターキーの代わりにメディアキーを使用すればよい。

次にＳ３２０６に進み、その一回の記録ごとに固有の鍵：タイトルキー(Title Key）をランダムに、あるいはあからじめ定められた方法で生成し、ディスクに記録する。

ディスク上には、どこのデータがどんなタイトルを構成するかという情報が格納されたデータ管理ファイルがあり、このファイルにタイトルキーを格納することができる。

ステップＳ３２０７乃至Ｓ３２１５は図２９のＳ１８０７乃至Ｓ１８１５と同様であるため説明を省略する。

さらに、ステップＳ３２１６、Ｓ３２１７において、この記録処理に係るコンテンツに対応する著作権情報（Copyright Information）を生成し、さらに、その改竄チェック値としてのＭＡＣ（Message Authentication Code）を生成して、ディスクに著作権情報＆ＭＡＣを記録する。前述したように、著作権情報(Copyright Information）は、例えば、入力ソース情報、記録機器の電子透かし世代情報（前述の第１、２，３世代)、記録モードの各情報、コンテンツ中から取得されるコピー制御情報としてのＣＣＩから選択された最も厳しい最厳格コピー制御情報であるタイトル別コピー制御情報、さらに、記録コンテンツにおけるコピー制御情報の変化点を示す情報としての対応パケットナンバーと変化点におけるコピー制御情報などであり、これらの情報中から１以上の情報を著作権情報として設定して記録媒体に格納する。著作権情報の生成処理例は、先に、図２５、図２６、図２７を参照して説明した通りであり、ＭＡＣ生成処理は、図２８を用いて説明した処理にしたがって実行される。

上述の処理にしたがって、コンテンツに対応して記録媒体に著作権情報が格納され、再生、出力時に記録媒体に格納された暗号化コンテンツの復号を行なうことなく著作権情報を取得することが可能となり、再生制御、出力制御が正しく実行される。また、記録媒体を他の再生装置に設定して再生する場合においても、著作権情報に格納されたソース情報、あるいは電子透かし世代情報を参照することにより、コンテンツ記録機器において設定されたコピー制御情報を正しく判定することが可能となるので、正しい再生制御が実行される。

なお、上記の説明では、メディアキー（Media Key）とスタンパーＩＤ(Stamper ID)とディスクＩＤ（Disc ID）からディスク固有キー（Disc Unique Key）を生成し、これとタイトルキー（Title Key）と データ解析記録方式用キー（Cognizant Key)もしくはデータ非解析記録方式用キー（Non-Cognizant Key)からタイトル固

有キー（Title Unique Key）をそれぞれ生成するようにしているが、ディスク固有キー（Disc Unique Key）を不要としてメディアキー（Media Key）と スタンパーＩＤ(Stamper ID)とディスクＩＤ（Disc ID）とタイトルキー（Title Key）と、データ解析記録方式用キー（Cognizant Key)もしくはデータ非解析記録方式用キー（Non-Cognizant Key)から直接タイトル固有キー（Title Unique Key）を生成してもよく、また、タイトルキー（Title Key）を用いずに、メディアキー（Media Key）と スタンパーＩＤ(Stamper ID)とディスクＩＤ（Disc ID）と、データ解析記録方式用キー（Cognizant Key)もしくはデータ非解析記録方式用キー（Non-Cognizant Key)からタイトル固有キー（Title Unique Key）相当の鍵を生成してもよい。

以上のようにして、メディアキーを用いて記録媒体にデータを記録することができる。

次に、上記のようにして記録されたデータを再生する処理について、図４６のブロック図と図４７のフローチャートを用いて説明する。

図４６は、第１の実施例における図３１に対応する図であり、マスターキー（Master Key）の変わりにメディアキー（Media Key）が使われ、そのため記録時世代番号（Generation #）が省略されている点が異なっている。

図４７のＳ３４０１において、記録再生装置３４００は記録媒体であるディスク３４２０からスタンパーＩＤ(Stamper ID)およびディスクＩＤ（Disc ID）を、また自身のメモリからデータ解析記録方式用キー（Cognizant Key)および／あるいはデータ非解析記録方式用キー（Non-Cognizant Key)と、図４１のＳ２８０４で計算し一時的に保存しているメディアキーを読み出す。

なお、この記録媒体の挿入時に、図４１の処理を行い、メディアキーを入手できなかった場合には、再生処理を行わずに終了する。

次にＳ３４０２で、ディスクから読み出すべきデータのタイトルキー（Title Key）とこのコンテンツデータに対応して記録され、改竄チェックデータとしてのＭＡＣの付加された著作権情報を読み出す。著作権情報(Copyright Information)には、コンテンツの入力ソース情報、記録機器の電子透かし世代情報（前述の第１、２，３世代)、記録モードの各情報と、コンテンツ中から取得されるコピー制

御情報であるＣＣＩから選択された最も厳しい最厳格コピー制御情報としてのタイトル別コピー制御情報、さらに、記録コンテンツにおけるコピー制御情報の変化点を示す情報としての対応パケットナンバーと変化点におけるコピー制御情報中から１以上の情報が含まれる。また、著作権情報（Copyright Information）は、容易に改ざんされないように、正当性検査コードとしてのＭＡＣ（Message Authentication Code）が付加されている。

ステップＳ３４０３では、ディスクＩＤ（Disc ID）とメディアキーとスタンパーＩＤ(Stamper ID)を用いてディスク固有キー（Disc Unique Key）を生成する。このキー生成方法は、先に図２１を用いて説明した処理において、マスターキーをメデイアキーに置き換えることで実現される。例えば、FIPS 180-1で定められているハッシュ関数 SHA-1に、メディアキーとディスクＩＤ（Disc ID）とのビット連結により生成されるデータを入力し、その１６０ビットの出力から必要なデータ長のみをディスク固有キー（Disc Unique Key）として使用する方法や、ブロック暗号関数を用いたハッシュ関数にメディアキーとディスクＩＤ（Disc ID）を入力して得られた結果を用いるなどの方法が挙げられる。

次に、ステップＳ３４０４において、著作権情報のＭＡＣの計算を実行する。ＭＡＣ計算は、先に図２８を用いて説明した処理によって実行され、図２８に示すように、６４ビットブロック暗号関数を用いたハッシュ関数にディスク固有キーとタイトルキーと著作権情報を入力して得られた結果を用いる例１の方法や、FIPS 180-1で定められているハッシュ関数ＳＨＡ－１に、ディスク固有キーとタイトルキーと著作権情報とのビット連結により生成されるデータを入力し、その１６０ビットの出力から必要なデータ長のみを著作権情報ＭＡＣ値として使用する例２の方法が適用できる。

著作権情報とともに記録媒体に格納されたＭＡＣ値と、読み出した著作権情報に基づいて新たに生成したＭＡＣ値とが等しいと判断されれば、著作権情報の改竄はないものと判断される。

ステップＳ３４０５では、このＭＡＣ判定を含む判定結果に基づいて再生可能性の判定が実行される。判定処理の詳細フローを図４８に示す。

ステップＳ３５０１ではメディアキー（Media Key）を得られたか否かを判定す

る。メディアキーを得られなかった場合、再生不可能となり、メディアキーを得られた場合はステップＳ３５０２に進む。ステップＳ３５０２の処理は図３３のＳ２５０３と同じであり、そのデータの記録時に使われた記録モードに対応する鍵（データ解析記録方式（Cognizant Mode)の場合、データ解析記録方式用キー（Cognizant Key),データ非解析記録方式（Non-Cognizant Mode)の場合、データ非解析記録方式用キー（Non-Cognizant Key)）を再生機器が持っている場合には、ステップＳ３５０３に進む。

ステップＳ３５０３では、図３２のステップＳ３４０４で計算したＭＡＣが正しいか否か、すなわち、記録媒体に格納されたＭＡＣと計算値としてのＭＡＣが等しいか否かが判定される。等しい場合は、ステップＳ３５０５に進み、不一致の場合は、著作権情報に改竄ありと判定されて再生不可能の処理となる。

ステップＳ３５０５では、記録媒体から読み出した著作権情報の検討が実行され、著作権情報に基づいて再生の可否が判定される。

著作権情報には、前述したように様々な態様の情報格納形態があり、その情報形態によって、前述の図３４に示した入力ソース情報に基づく再生可否判定処理、図３５に示した電子透かし世代情報に基づく再生可否判定処理、図３６に示した著作権情報中のタイトル別コピー制御情報に基づく再生可否判定処理の少なくともいずれかの処理が実行されることになる。再生予定のコンテンツに対応して記録媒体に格納された著作権情報に複数の情報が含まれる場合は、複数の情報に基づく判定処理をシーケンシャルにあるいはパラレルに実行して、すべての判定において再生可と判定された場合においてのみ最終的に再生可と判定し、いずれかの判定において、１つでも再生不可の判定がなされた場合には、再生不可とする処理を行なう構成とする。

これらの判定の結果に基づいて、図４８の再生可能性の判定処理が終了し、すべての条件が満足し、再生可能と判定されれば、図４７に示すステップＳ３４０６に移行する。なお、前述したように電子透かしの判定処理が復号データに対する電子透かし検出に基づいて実行される場合は、電子透かしに基づく再生可能性の判定は、図４７のステップＳ３４０９のブロックデータの復号処理の後に実行する。

図４７のフローのその後の処理、ステップＳ３４０６乃至Ｓ３４１０の処理は、図３２のＳ２４０６乃至Ｓ２４１０と同様であるため、説明を省略する。

なお、上記の説明では、メディアキー（Media Key）と スタンパーＩＤ(Stamper ID)とディスクＩＤ（Disc ID）からディスク固有キー（Disc Unique Key）を生成し、これとタイトルキー（Title Key）と、データ解析記録方式用キー（Cognizant Key)もしくはデータ非解析記録方式用キー（Non-Cognizant Key)からタイトル固有キー（Title Unique Key）をそれぞれ生成するようにしているが、ディスク固有キー（Disc Unique Key）を不要としてメディアキー（Media Key）と スタンパーＩＤ(Stamper ID)とディスクＩＤ（Disc ID）とタイトルキー（Title Key）と、データ解析記録方式用キー（Cognizant Key)もしくはデータ非解析記録方式用キー（Non-Cognizant Key)から直接タイトル固有キー（Title Unique Key）を生成してもよく、また、タイトルキー（Title Key）を用いずに、メディアキー（Media Key）と スタンパーＩＤ(Stamper ID)とディスクＩＤ（Disc ID）と、データ解析記録方式用キー（Cognizant Key)もしくはデータ非解析記録方式用キー（Non-Cognizant Key)からタイトル固有キー（Title Unique Key）相当の鍵を生成してもよい。

上記のようにして、記録媒体へのデータの記録および記録媒体からの再生処理が実行される。

上述したように、本発明の情報処理装置としての再生装置は、コンテンツの再生に際し、コンテンツに対応して生成格納された著作権情報に基づいて再生、出力の可否を判定する。著作権情報には、入力ソース情報、記録機器の電子透かし世代情報（前述の第１、２，３世代)、記録モードの各情報、コンテンツ中から取得されるコピー制御情報としてのＣＣＩから選択された最も厳しい最厳格コピー制御情報であるタイトル別コピー制御情報、さらに、記録コンテンツにおけるコピー制御情報の変化点を示す情報としての対応パケットナンバーと変化点におけるコピー制御情報などであり、これらの情報中から１以上の情報を取得して再生の可否を判定する。

［９．記録再生装置ハードウェア構成］

上述した一連の処理を実行する記録再生装置としての情報処理装置構成例につ

いて説明する。上述した各フロー、ブロック図を参照して説明した処理はハードウェア、ソフトウェアの組合わせにより実行可能である。例えば、記録再生装置における暗号処理手段は暗号化／復号ＬＳＩとして構成することも可能であるが、汎用のコンピュータや、１チップのマイクロコンピュータにプログラムを実行させることにより行う構成とすることができる。同様にＴＳ処理手段も処理をソフトウェアによって実行することが可能である。一連の処理をソフトウェアによって行う場合には、そのソフトウェアを構成するプログラムが、汎用のコンピュータや１チップのマイクロコンピュータ等にインストールされる。図４９は、上述した一連の処理を実行するプログラムがインストールされるコンピュータの一実施の形態の構成例を示している。

プログラムは、コンピュータに内蔵されている記録媒体としてのハードディスク４２０５やＲＯＭ４２０３に予め記録しておくことができる。あるいは、プログラムはフロッピーディスク、ＣＤ－ＲＯＭ(Compact Disc Read Only Memory)，ＭＯ(Magneto optical)ディスク，ＤＶＤ(Digital Versatile Disc)、磁気ディスク、半導体メモリなどのリムーバブル記録媒体４２１０に、一時的あるいは永続的に格納（記録）しておくことができる。このようなリムーバブル記録媒体４２１０は、いわゆるパッケージソフトウエアとして提供することができる。

なお、プログラムは、上述したようなリムーバブル記録媒体４２１０からコンピュータにインストールする他、ダウンロードサイトから、デジタル衛星放送用の人工衛星を介して、コンピュータに無線で転送したり、ＬＡＮ(Local Area Network)、インターネットといったネットワークを介して、コンピュータに有線で転送し、コンピュータでは、そのようにして転送されてくるプログラムを、通信部４２０８で受信し、内蔵するハードディスク４２０５にインストールすることができる。

コンピュータは、ＣＰＵ(Central Processing Unit)４２０２を内蔵している。ＣＰＵ４２０２には、バス４２０１を介して、入出力インタフェース４２１１が接続されており、ＣＰＵ４２０２は、入出力インタフェース４２１０を介して、ユーザによって、キーボードやマウス等で構成される入力部４２０７が操作されることにより指令が入力されると、それにしたがって、ＲＯＭ(Read Only Memory)

４２０３に格納されているプログラムを実行する。

あるいは、ＣＰＵ４２０２は、ハードディスク４２０５に格納されているプログラム、衛星若しくはネットワークから転送され、通信部４２０８で受信されてハードディスク４２０５にインストールされたプログラム、またはドライブ４２０９に装着されたリムーバブル記録媒体４２１０から読み出されてハードディスク４２０５にインストールされたプログラムを、ＲＡＭ(Random Access Memory)４２０４にロードして実行する。

これにより、ＣＰＵ４２０２は、上述したフローチャートにしたがった処理、あるいは上述したブロック図の構成により行われる処理を行う。そして、ＣＰＵ４２０２は、その処理結果を、必要に応じて、例えば、入出力インタフェース４２１１を介して、ＬＣＤ(Liquid Crystal Display)やスピーカ等で構成される出力部４２０６から出力、あるいは、通信部４２０８から送信、さらには、ハードディスク４２０５に記録させる。

ここで、本明細書において、コンピュータに各種の処理を行わせるためのプログラムを記述する処理ステップは、必ずしもフローチャートとして記載された順序に沿って時系列に処理する必要はなく、並列的あるいは個別に実行される処理（例えば、並列処理あるいはオブジェクトによる処理）も含むものである。

また、プログラムは、１のコンピュータにより処理されるものであっても良いし、複数のコンピュータによって分散処理されるものであっても良い。さらに、プログラムは、遠方のコンピュータに転送されて実行されるものであっても良い。

なお、本実施の形態では、コンテンツの暗号化／復号を行うブロックを、１チップの暗号化／復号ＬＳＩで構成する例を中心として説明したが、コンテンツの暗号化／復号を行うブロックは、例えば、図１および図２に示すＣＰＵ１７０が実行する１つのソフトウェアモジュールとして実現することも可能である。同様に、ＴＳ処理手段３００の処理もＣＰＵ１７０が実行する１つのソフトウェアモジュールとして実現することが可能である。

以上、特定の実施例を参照しながら、本発明について詳解してきた。しかしながら、本発明の要旨を逸脱しない範囲で当業者が該実施例の修正や代用を成し得ることは自明である。実施例においては、例示という形態で本発明を開示してき

たのであり、限定的に解釈されるべきではない。本発明の要旨を判断するためには、冒頭に記載した特許請求の範囲の欄を参酌すべきである。

産業上の利用可能性

上述したように、本発明の構成においては、記録媒体に格納するコンテンツに対応させてコンテンツに関する著作権情報を格納する構成とし、著作権情報として、記録コンテンツの入力ソース情報を格納する構成としたので、記録コンテンツの再生、出力に際して、再生対象コンテンツの入力ソース情報の取得が可能となり、取得した入力ソース情報に基づいて、再生、出力の可否を判定することが可能となる。

また、本発明の構成においては、記録媒体に格納するコンテンツに対応させてコンテンツに関する著作権情報を格納する構成とし、著作権情報として、記録コンテンツの入力ソース情報を格納し、記録再生装置のメモリに格納した出力制限情報との対応により、再生処理制御を実行する構成としたので、入力ソースに応じた正確な再生、出力制御を実行することが可能となる。

また、本発明の構成によれば、記録媒体に格納するコンテンツに対応させてコンテンツに関する著作権情報を格納する構成とし、著作権情報に対する改竄チェック値としてのＭＡＣを併せて格納する構成としたので、著作権情報の信頼性を維持することが可能となる。また、著作権情報に対する改竄チェック値としてのＭＡＣの生成用キーとして、用いるディスク固有キーを生成するのに必要なキーをツリー（木）構造の鍵配布構成に従った有効化キーブロック（ＥＫＢ）とともに送信し、送信したＥＫＢの処理により、正当なライセンスを受けたデバイスにおいてのみ取得可能なマスターキー、メディアキーを適用する構成としたので、正当なライセンス・デバイスにおいてのみＭＡＣ検証が可能となり、コンテンツの正当な利用構成が実現される。

請求の範囲

1．　コンテンツの記録媒体に対する記録処理を実行する情報記録装置であり、
記録媒体に対する記録対象コンテンツに関する入力ソース情報を含む著作権情報を生成し、前記記録対象コンテンツを格納する記録媒体に格納する処理を実行する構成を有することを特徴とする情報記録装置。

2．　前記情報記録装置は、
前記入力ソース情報を含む著作権情報に対応する改竄チェック用データを生成し、記録媒体に対して格納する著作権情報とともに格納する構成を有することを特徴とする請求項1に記載の情報記録装置。

3．　前記入力ソース情報は、ＩＥＥＥ１３９４インタフェースを介するコピー制御情報を持つコンテンツ入力であるか否かを示す情報を含むことを特徴とする請求項1に記載の情報記録装置。

4．　前記入力ソース情報は、デジタルデータ入力であるかアナログデータ入力であるかを示す情報を含むことを特徴とする請求項1に記載の情報記録装置。

5．　前記入力ソース情報は、入力コンテンツに対して設定されたコピー制御情報態様を含み、デジタルデータとしてのＴＳパケットに付加されたコピー制御情報を有するか、または電子透かしとして付加されたコピー制御情報を有するかを示す情報を含むことを特徴とする請求項1に記載の情報記録装置。

6．　前記情報記録装置は、
複数の異なる情報記録装置をリーフとした階層ツリー構造を構成する各ノードに固有のノードキーと各情報記録装置固有のリーフキーとを格納し、
ノードキーを下位階層のノードキーまたはリーフキーの少なくともいずれかを

含むキーにより暗号化した有効化キーブロック（ＥＫＢ）の復号処理を実行し、該復号処理によって取得可能な鍵を適用して、前記入力ソース情報を含む著作権情報に対応する改竄チェック用データを生成し、記録媒体に対して格納する著作権情報とともに格納する構成を有することを特徴とする請求項１に記載の情報記録装置。

７．　前記情報記録装置は、

複数の異なる情報記録装置をリーフとした階層ツリー構造を構成する各ノードに固有のノードキーと各情報記録装置固有のリーフキーとを格納し、

ノードキーを下位階層のノードキーまたはリーフキーの少なくともいずれかを含むキーにより暗号化した有効化キーブロック（ＥＫＢ）の復号処理を実行し、該復号処理によって取得可能な鍵を適用して、前記入力ソース情報を含む著作権情報に対応する改竄チェック用データを生成し、記録媒体に対して格納する著作権情報とともに格納する構成を有するとともに、

前記有効化キーブロック（ＥＫＢ）の復号処理を実行し、該復号処理によって取得可能な鍵を適用して取得される鍵に基づいて、記録対象コンテンツの暗号化処理を実行して記録媒体に対して格納する処理を実行する構成を有することを特徴とする請求項１に記載の情報記録装置。

８．　コンテンツの記録媒体からの再生処理を実行する情報再生装置であり、

記録媒体からの再生対象コンテンツに関する入力ソース情報を含む著作権情報を、前記再生対象コンテンツ格納記録媒体から読み出して、前記再生対象コンテンツの入力ソース情報に対応した出力制限に基づく再生制御を行なう構成を有することを特徴とする情報再生装置。

９．　前記情報再生装置は、

前記入力ソース情報を含む著作権情報に対応する改竄チェック用データを、前記再生対象コンテンツ格納記録媒体から読み出した著作権情報に基づいて生成し、該生成データと、前記記録媒体に格納済みの改竄チェック値との照合により、著

作権情報の改竄検証を実行し、改竄無しの結果取得を条件として、コンテンツ再生処理を実行する構成を有することを特徴とする請求項８に記載の情報再生装置。

１０．　前記入力ソース情報は、ＩＥＥＥ１３９４インタフェースを介するコピー制御情報を持つコンテンツ入力であるか否かを示す情報を含むことを特徴とする請求項８に記載の情報再生装置。

１１．　前記入力ソース情報は、デジタルデータ入力であるかアナログデータ入力であるかを示す情報を含むことを特徴とする請求項８に記載の情報再生装置。

１２．　前記入力ソース情報は、入力コンテンツに対して設定されたコピー制御情報態様を含み、デジタルデータとしてのＴＳパケットに付加されたコピー制御情報を有するか、または電子透かしとして付加されたコピー制御情報を有するかを示す情報を含むことを特徴とする請求項８に記載の情報再生装置。

１３．　前記情報再生装置は、

複数の異なる情報再生装置をリーフとした階層ツリー構造を構成する各ノードに固有のノードキーと各情報再生装置固有のリーフキーとを格納し、

ノードキーを下位階層のノードキーまたはリーフキーの少なくともいずれかを含むキーにより暗号化した有効化キーブロック（ＥＫＢ）の復号処理を実行し、該復号処理によって取得可能な鍵を適用して、前記入力ソース情報を含む著作権情報に対応する改竄チェック用データを生成し、著作権情報の改竄検証を実行する構成を有することを特徴とする請求項８に記載の情報再生装置。

１４．　前記情報再生装置は、

複数の異なる情報再生装置をリーフとした階層ツリー構造を構成する各ノードに固有のノードキーと各情報再生装置固有のリーフキーとを格納し、

ノードキーを下位階層のノードキーまたはリーフキーの少なくともいずれかを含むキーにより暗号化した有効化キーブロック（ＥＫＢ）の復号処理を実行し、

該復号処理によって取得可能な鍵を適用して、前記入力ソース情報を含む著作権情報に対応する改竄チェック用データを生成し、著作権情報の改竄検証を実行する構成を有するとともに、

前記有効化キーブロック（ＥＫＢ）の復号処理を実行し、該復号処理によって取得可能な鍵を適用して取得される鍵に基づいて、再生対象コンテンツの復号処理を実行して記録媒体からのコンテンツ再生処理を実行する構成を有することを特徴とする請求項８に記載の情報再生装置。

１５．コンテンツの記録媒体に対する記録処理を実行する情報記録方法であり、

記録媒体に対する記録対象コンテンツに関する入力ソース情報を含む著作権情報を生成し、前記記録対象コンテンツを格納する記録媒体に格納する処理を実行することを特徴とする情報記録方法。

１６．前記情報記録方法は、さらに、

前記入力ソース情報を含む著作権情報に対応する改竄チェック用データを生成し、記録媒体に対して格納する著作権情報とともに格納することを特徴とする請求項１５に記載の情報記録方法。

１７．前記入力ソース情報は、ＩＥＥＥ１３９４インタフェースを介するコピー制御情報を持つコンテンツ入力であるか否かを示す情報を含むことを特徴とする請求項１５に記載の情報記録方法。

１８．前記入力ソース情報は、デジタルデータ入力であるかアナログデータ入力であるかを示す情報を含むことを特徴とする請求項１５に記載の情報記録方法。

１９．前記入力ソース情報は、入力コンテンツに対して設定されたコピー制御情報態様を含み、デジタルデータとしてのＴＳパケットに付加されたコピー制御情報を有するか、または電子透かしとして付加されたコピー制御情報を有するかを示す情報を含むことを特徴とする請求項１５に記載の情報記録方法。

２０．　前記情報記録方法を実行する情報記録装置は、複数の異なる情報記録装置をリーフとした階層ツリー構造を構成する各ノードに固有のノードキーと各情報記録装置固有のリーフキーとを格納し、前記情報記録方法において、

ノードキーを下位階層のノードキーまたはリーフキーの少なくともいずれかを含むキーにより暗号化した有効化キーブロック（ＥＫＢ）の復号処理を実行し、該復号処理によって取得可能な鍵を適用して、前記入力ソース情報を含む著作権情報に対応する改竄チェック用データを生成し、記録媒体に対して格納する著作権情報とともに格納する処理を実行することを特徴とする請求項１５に記載の情報記録方法。

２１．　前記情報記録方法を実行する情報記録装置は、複数の異なる情報記録装置をリーフとした階層ツリー構造を構成する各ノードに固有のノードキーと各情報記録装置固有のリーフキーとを格納し、前記情報記録方法において、

ノードキーを下位階層のノードキーまたはリーフキーの少なくともいずれかを含むキーにより暗号化した有効化キーブロック（ＥＫＢ）の復号処理を実行し、該復号処理によって取得可能な鍵を適用して、前記入力ソース情報を含む著作権情報に対応する改竄チェック用データを生成し、記録媒体に対して格納する著作権情報とともに格納するとともに、

前記有効化キーブロック（ＥＫＢ）の復号処理を実行し、該復号処理によって取得可能な鍵を適用して取得される鍵に基づいて、記録対象コンテンツの暗号化処理を実行して記録媒体に対して格納する処理を実行することを特徴とする請求項１５に記載の情報記録方法。

２２．　コンテンツの記録媒体からの再生処理を実行する情報再生方法であり、

記録媒体からの再生対象コンテンツに関する入力ソース情報を含む著作権情報を、前記再生対象コンテンツ格納記録媒体から読み出して、前記再生対象コンテンツの入力ソース情報に対応した出力制限に基づく再生制御を行なうことを特徴とする情報再生方法。

２３．　前記情報再生方法は、さらに、

前記入力ソース情報を含む著作権情報に対応する改竄チェック用データを、前記再生対象コンテンツ格納記録媒体から読み出した著作権情報に基づいて生成し、該生成データと、前記記録媒体に格納済みの改竄チェック値との照合により、著作権情報の改竄検証を実行し、改竄無しの結果取得を条件として、コンテンツ再生処理を実行することを特徴とする請求項２２に記載の情報再生方法。

２４．　前記入力ソース情報は、ＩＥＥＥ１３９４インタフェースを介するコピー制御情報を持つコンテンツ入力であるか否かを示す情報を含むことを特徴とする請求項２２に記載の情報再生方法。

２５．　前記入力ソース情報は、デジタルデータ入力であるかアナログデータ入力であるかを示す情報を含むことを特徴とする請求項２２に記載の情報再生方法。

２６．　前記入力ソース情報は、入力コンテンツに対して設定されたコピー制御情報態様を含み、デジタルデータとしてのＴＳパケットに付加されたコピー制御情報を有するか、または電子透かしとして付加されたコピー制御情報を有するかを示す情報を含むことを特徴とする請求項２２に記載の情報再生方法。

２７．　前記情報再生方法を実行する情報再生装置は、複数の異なる情報再生装置をリーフとした階層ツリー構造を構成する各ノードに固有のノードキーと各情報再生装置固有のリーフキーとを格納し、前記情報再生方法において、

ノードキーを下位階層のノードキーまたはリーフキーの少なくともいずれかを含むキーにより暗号化した有効化キーブロック（ＥＫＢ）の復号処理を実行し、該復号処理によって取得可能な鍵を適用して、前記入力ソース情報を含む著作権情報に対応する改竄チェック用データを生成し、著作権情報の改竄検証を実行することを特徴とする請求項２２に記載の情報再生方法。

２８．　前記情報再生方法を実行する情報再生装置は、複数の異なる情報再生装置をリーフとした階層ツリー構造を構成する各ノードに固有のノードキーと各情報再生装置固有のリーフキーとを格納し、前記情報再生方法において、

ノードキーを下位階層のノードキーまたはリーフキーの少なくともいずれかを含むキーにより暗号化した有効化キーブロック（ＥＫＢ）の復号処理を実行し、該復号処理によって取得可能な鍵を適用して、前記入力ソース情報を含む著作権情報に対応する改竄チェック用データを生成し、著作権情報の改竄検証を実行するとともに、

前記有効化キーブロック（ＥＫＢ）の復号処理を実行し、該復号処理によって取得可能な鍵を適用して取得される鍵に基づいて、再生対象コンテンツの復号処理を実行して記録媒体からのコンテンツ再生処理を実行することを特徴とする請求項２２に記載の情報再生方法。

２９．　コンテンツの記録媒体に対する記録処理をコンピュータ・システム上で実行せしめるコンピュータ・プログラムであって、

記録媒体に対する記録対象コンテンツに関する入力ソース情報を含む著作権情報を生成するステップと、

前記記録対象コンテンツを格納する記録媒体に格納する処理ステップと、

を具備することを特徴とするコンピュータ・プログラム。

３０．　コンテンツの記録媒体からの再生処理をコンピュータ・システム上で実行せしめるコンピュータ・プログラムであって、

記録媒体からの再生対象コンテンツに関する入力ソース情報を含む著作権情報を、前記再生対象コンテンツ格納記録媒体から読み出すステップと、

前記再生対象コンテンツの入力ソース情報に対応した出力制限に基づく再生制御を行なうステップと、

を具備することを特徴とするコンピュータ・プログラム。

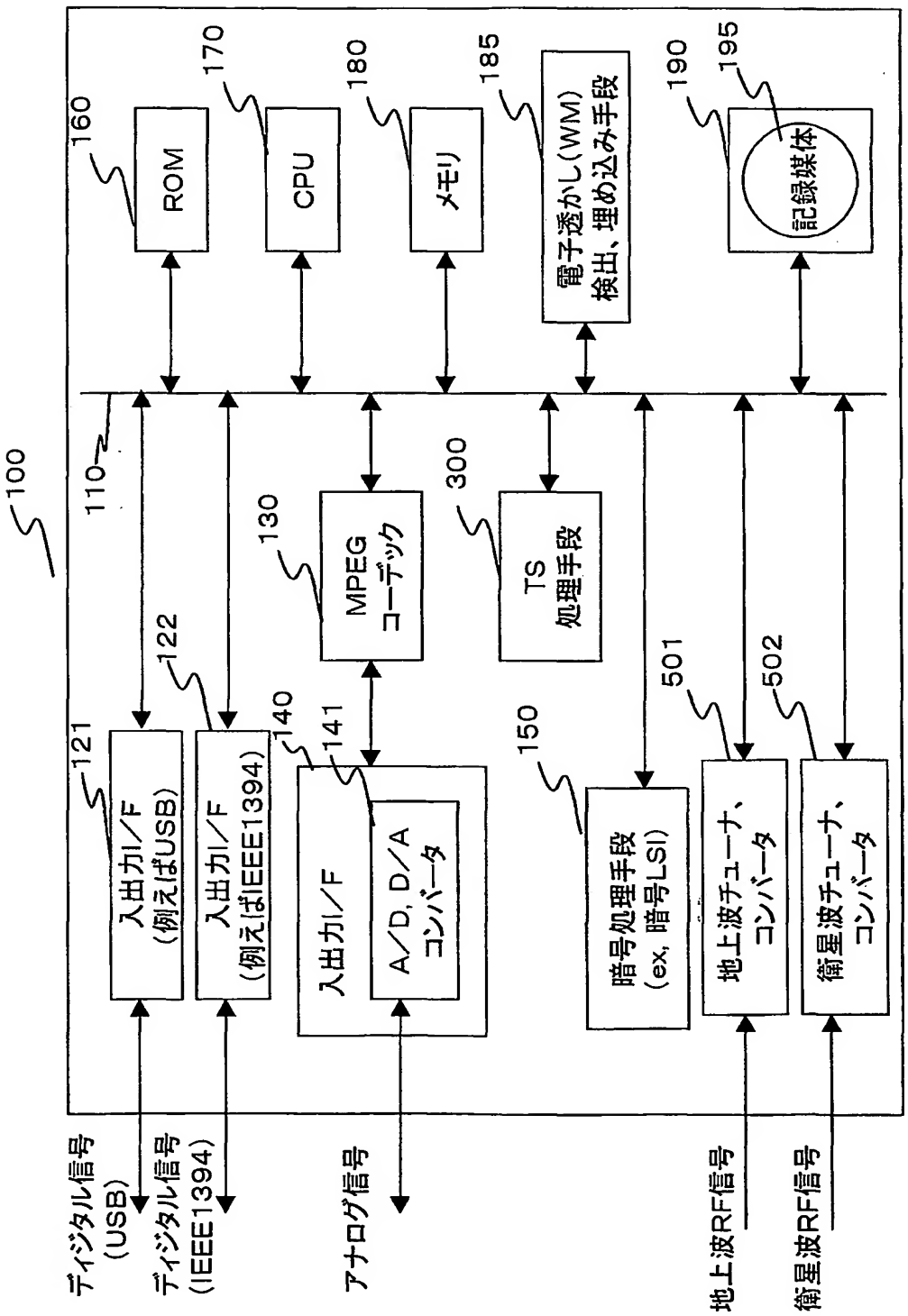

100
110
160
ROM
170
CPU
180
メモリ
185
電子透かし(WM)
検出、埋め込み手段
190
195
記録媒体
130
MPEG
コーデック
300
TS
処理手段
121
入出力I/F
(例えばUSB)
122
入出力I/F
(例えばIEEE1394)
140
141
入出力I/F
A/D, D/A
コンバータ
150
暗号処理手段
(ex, 暗号LSI)
501
地上波チューナ、
コンバータ
502
衛星波チューナ、
コンバータ
ディジタル信号
(USB)
ディジタル信号
(IEEE1394)
アナログ信号
地上波RF信号
衛星波RF信号

Fig.1

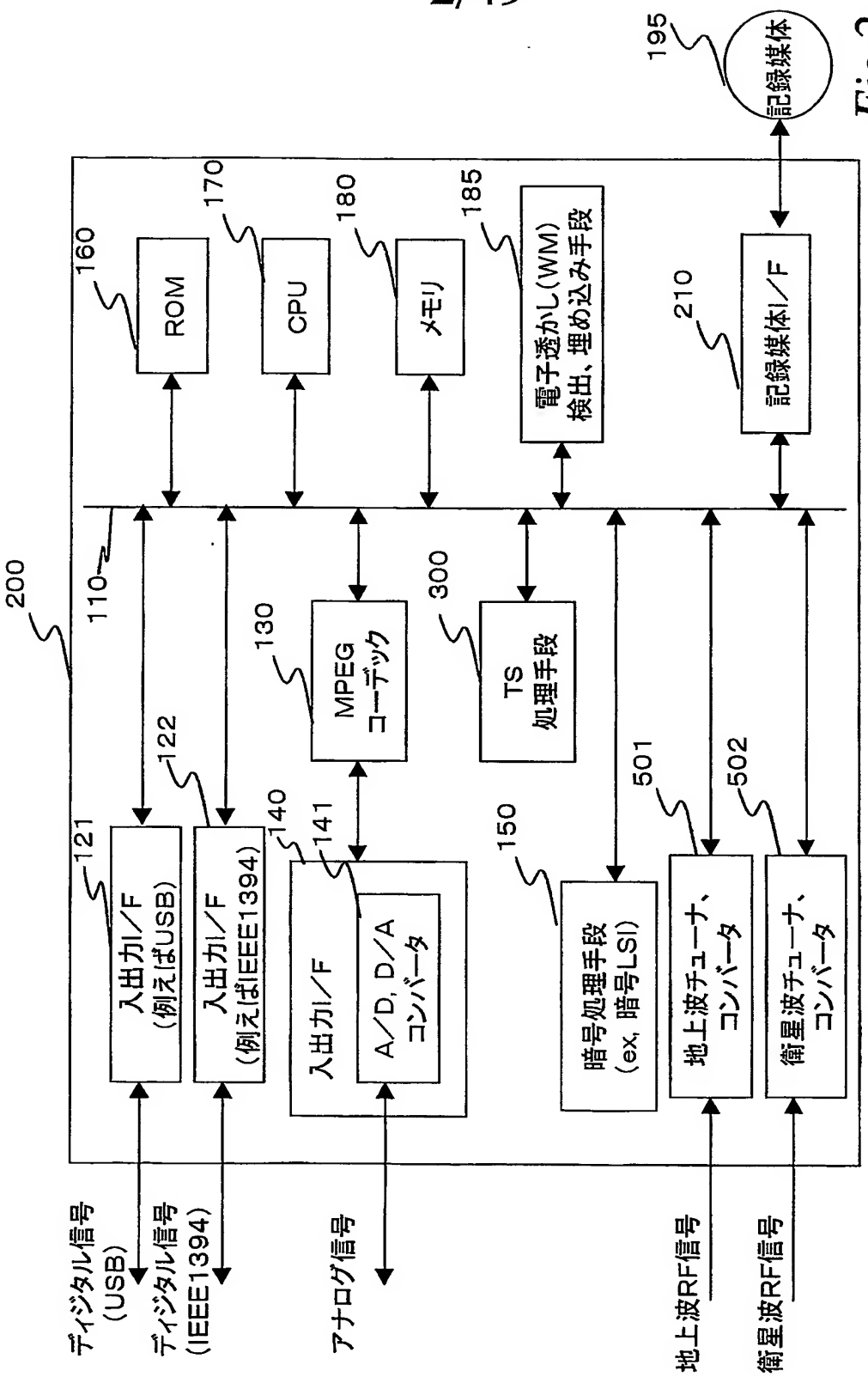

200
110
160
ROM
170
CPU
180
メモリ
185
電子透かし(WM)
検出、埋め込み手段
210
記録媒体I/F
195
記録媒体
121
入出力I/F
(例えばUSB)
122
入出力I/F
(例えばIEEE1394)
130
MPEG
コーデック
140
141
入出力I/F
A/D, D/A
コンバータ
300
TS
処理手段
150
暗号処理手段
(ex, 暗号LSI)
501
地上波チューナ、
コンバータ
502
衛星波チューナ、
コンバータ
ディジタル信号
(USB)
ディジタル信号
(IEEE1394)
アナログ信号
地上波RF信号
衛星波RF信号

Fig.2

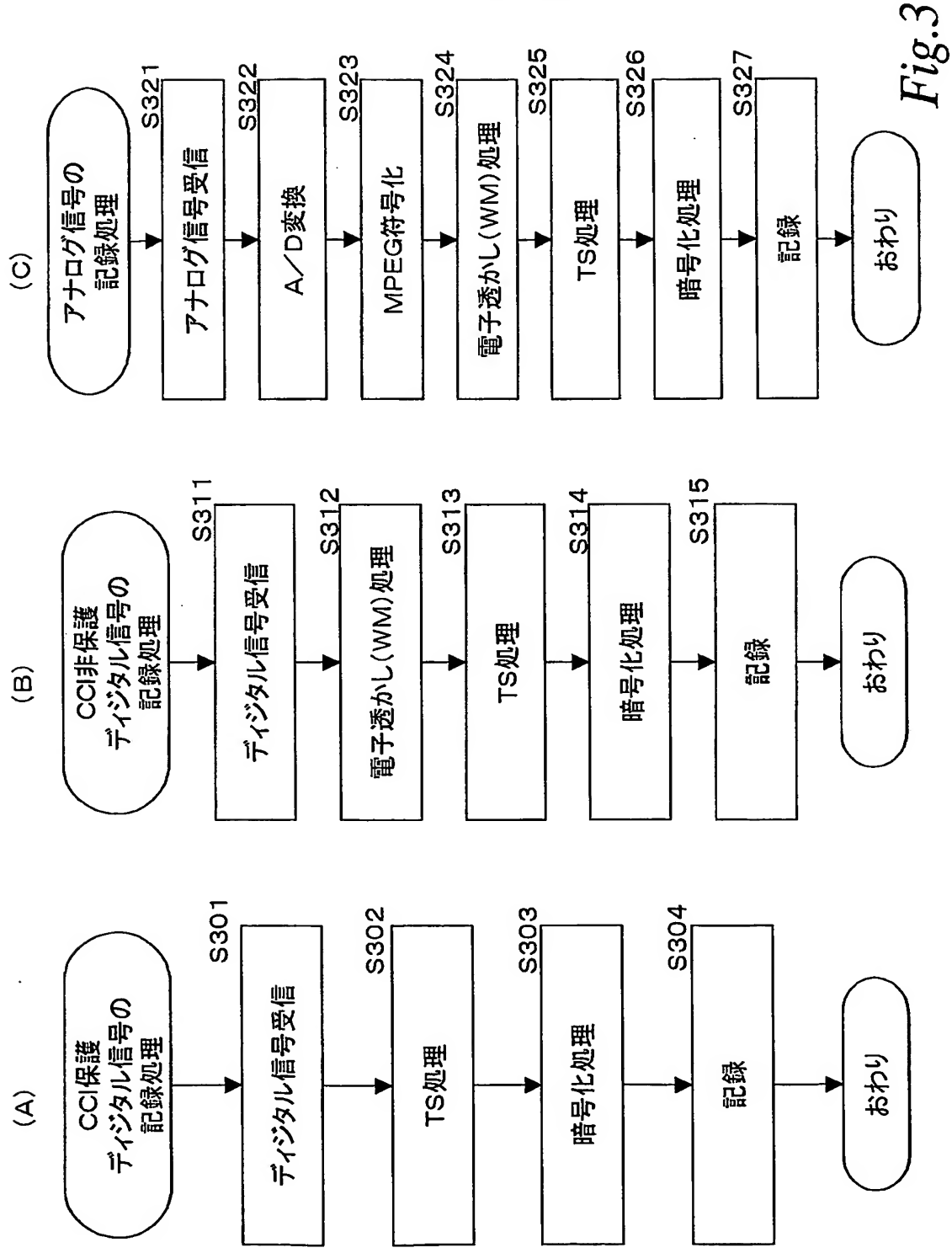

(A)
CCI保護
ディジタル信号の
記録処理
S301
ディジタル信号受信
S302
TS処理
S303
暗号化処理
S304
記録
おわり
(B)
CCI非保護
ディジタル信号の
記録処理
S311
ディジタル信号受信
S312
電子透かし(WM)処理
S313
TS処理
S314
暗号化処理
S315
記録
おわり
(C)
アナログ信号の
記録処理
S321
アナログ信号受信
S322
A/D変換
S323
MPEG符号化
S324
電子透かし(WM)処理
S325
TS処理
S326
暗号化処理
S327
記録
おわり

Fig.3

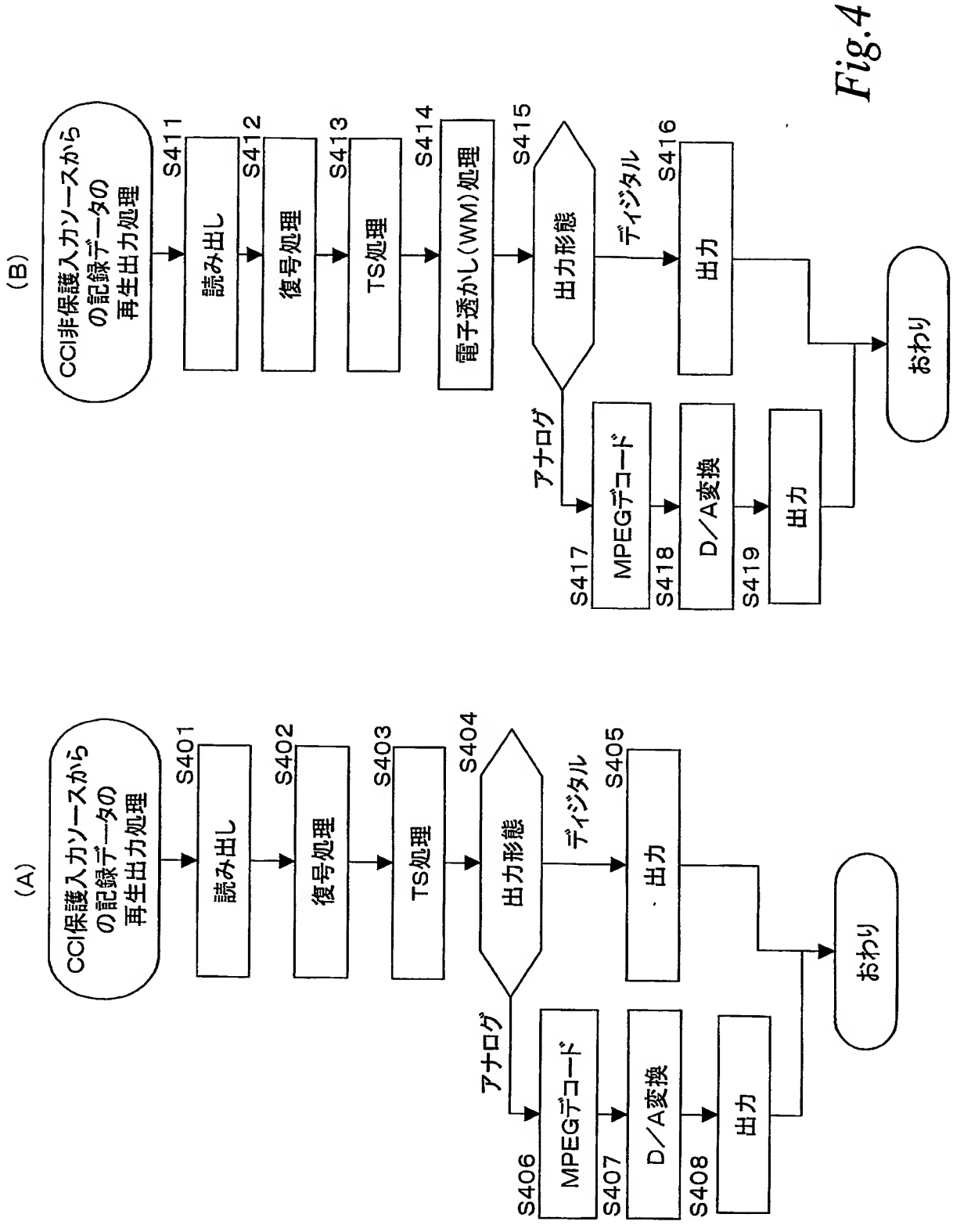

(A)
CCI保護入力ソースからの記録データの再生出力処理
S401
読み出し
S402
復号処理
S403
TS処理
S404
出力形態
アナログ
S406
MPEGデコード
S407
D／A変換
S408
出力
ディジタル
S405
出力
おわり
(B)
CCI非保護入力ソースからの記録データの再生出力処理
S411
読み出し
S412
復号処理
S413
TS処理
S414
電子透かし(WM)処理
S415
出力形態
アナログ
S417
MPEGデコード
S418
D／A変換
S419
出力
ディジタル
S416
出力
おわり

Fig.4

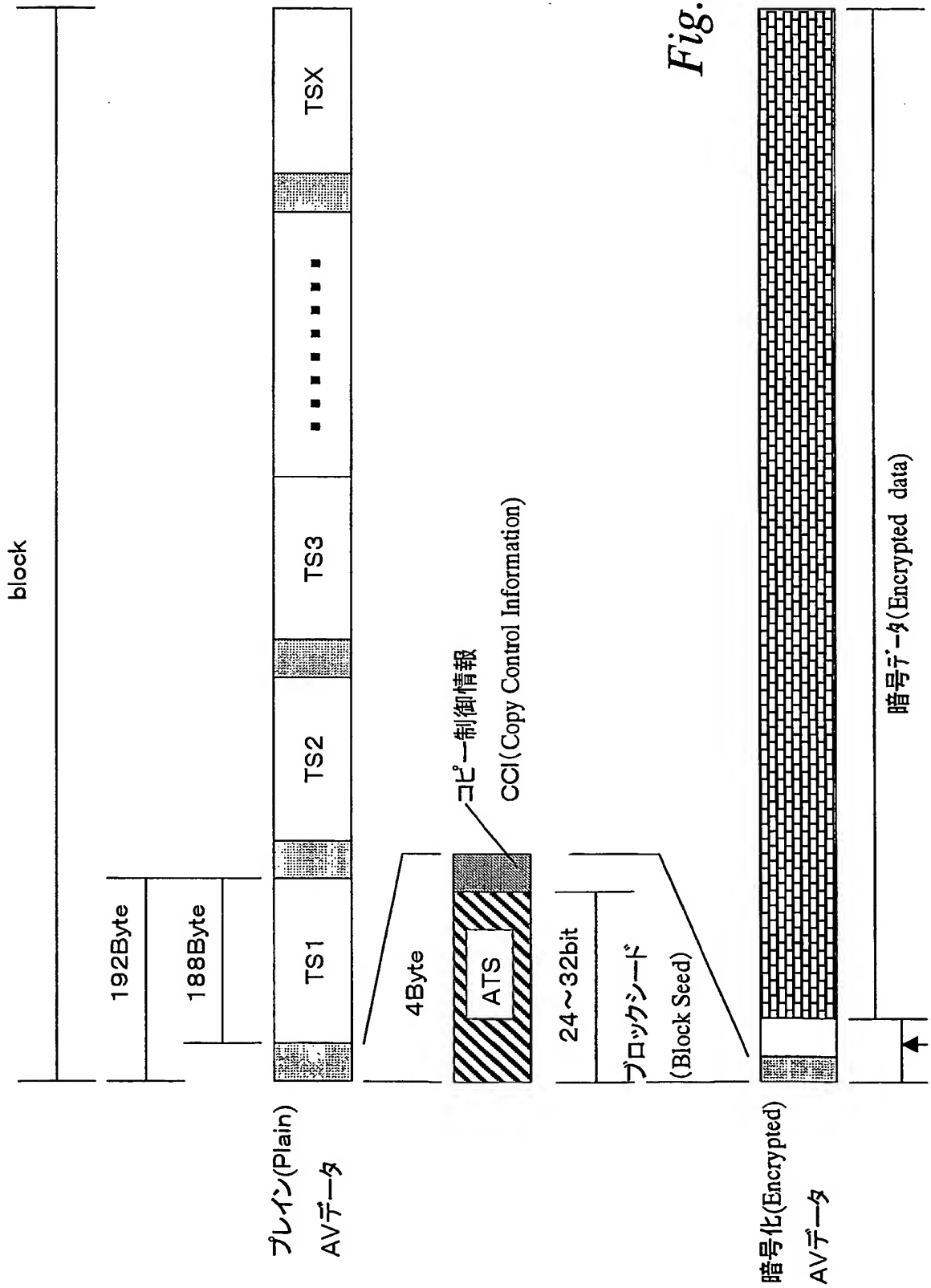

block
192Byte
188Byte
TS1
TS2
TS3
TSX
4Byte
ATS
コピー制御情報
CCI(Copy Control Information)
24～32bit
ブロックシード
(Block Seed)
プレイン(Plain)
AVデータ
暗号化(Encrypted)
AVデータ
暗号データ(Encrypted data)
非暗号データ(Unencrypted data)

Fig.5

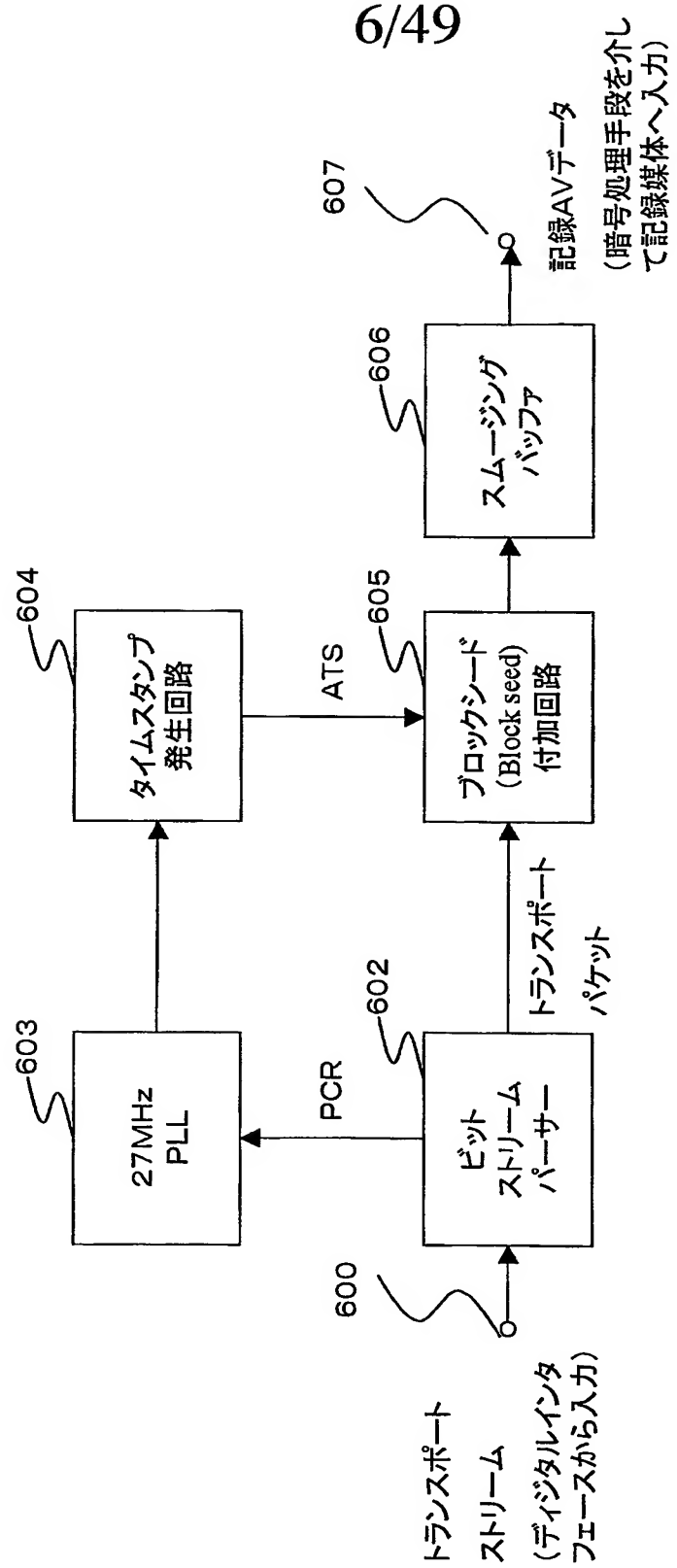

トランスポート
ストリーム
(ディジタルインタ
フェースから入力)
600
ビット
ストリーム
パーサー
602
PCR
27MHz
PLL
603
トランスポート
パケット
タイムスタンプ
発生回路
604
ATS
ブロックシード
(Block seed)
付加回路
605
スムージング
バッファ
606
607
記録AVデータ
(暗号処理手段を介し
て記録媒体へ入力)

Fig.6

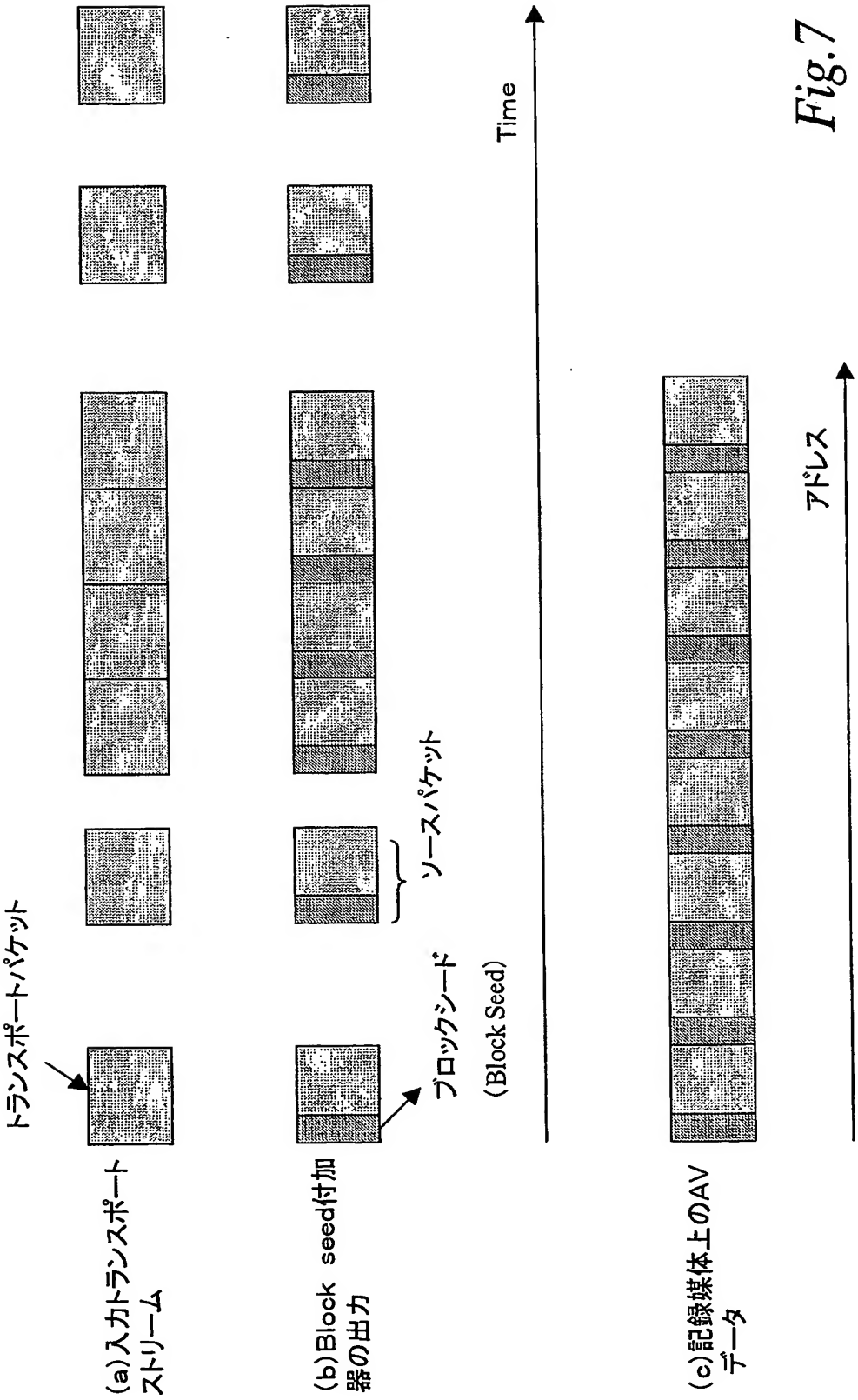

トランスポートパケット
(a)入力トランスポートストリーム
ブロックシード
(Block Seed)
ソースパケット
(b)Block seed付加器の出力
Time
(c)記録媒体上のAVデータ
アドレス

Fig.7

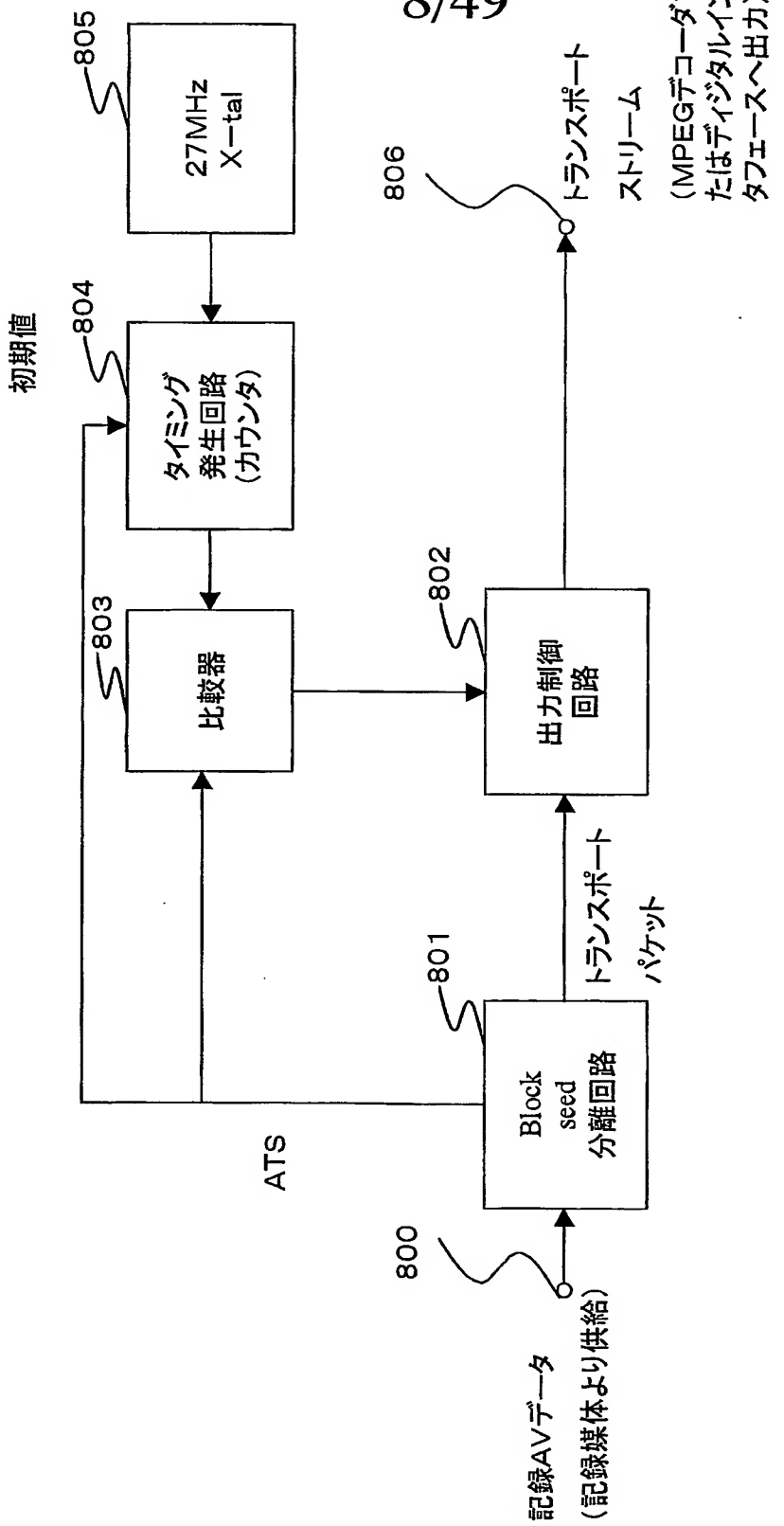

805
27MHz
X−tal
804
タイミング
発生回路
(カウンタ)
初期値
803
比較器
802
出力制御
回路
806
トランスポート
ストリーム
(MPEGデコーダまたはディジタルインタフェースへ出力)
801
Block
seed
分離回路
トランスポート
パケット
ATS
800
記録AVデータ
(記録媒体より供給)

Fig.8

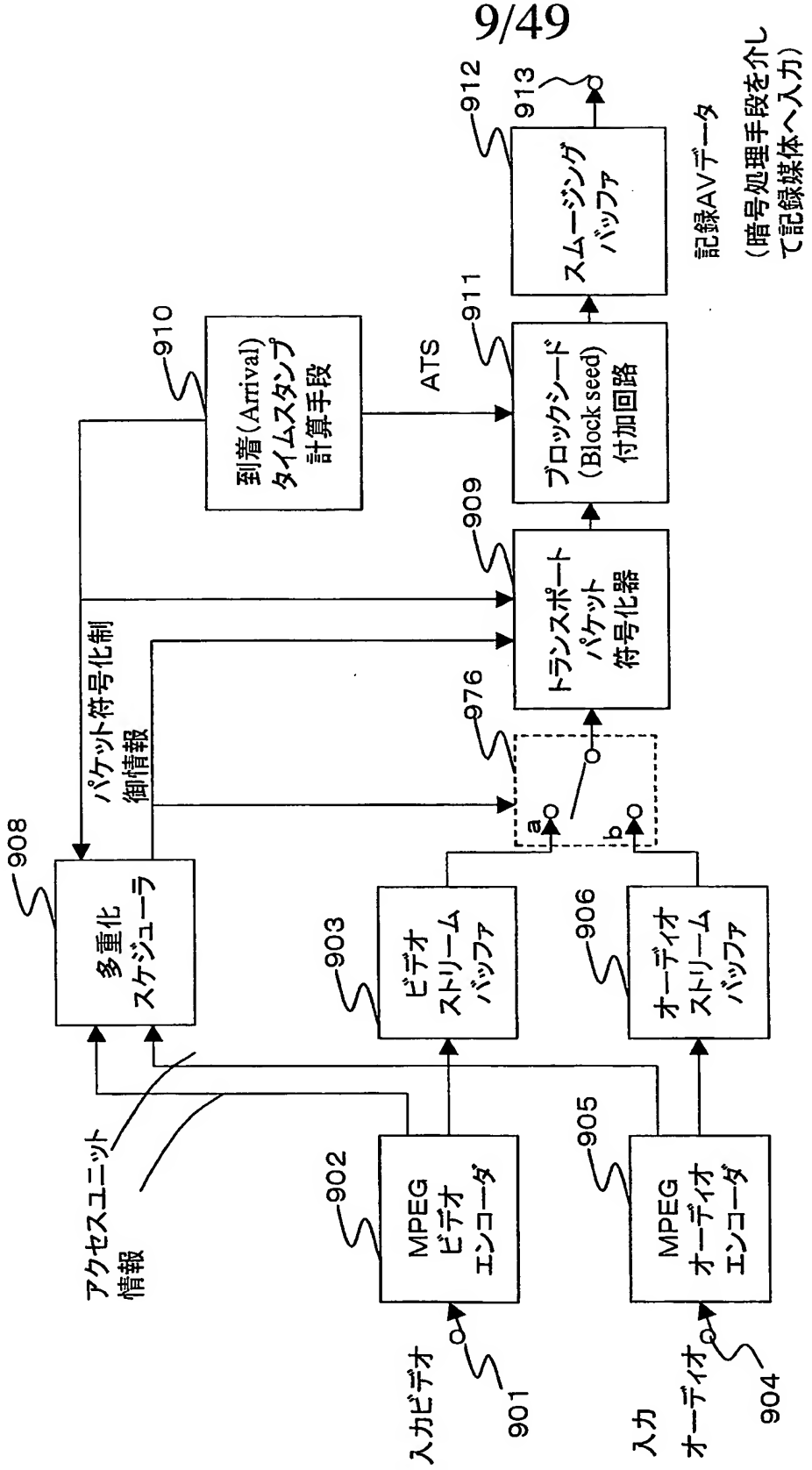
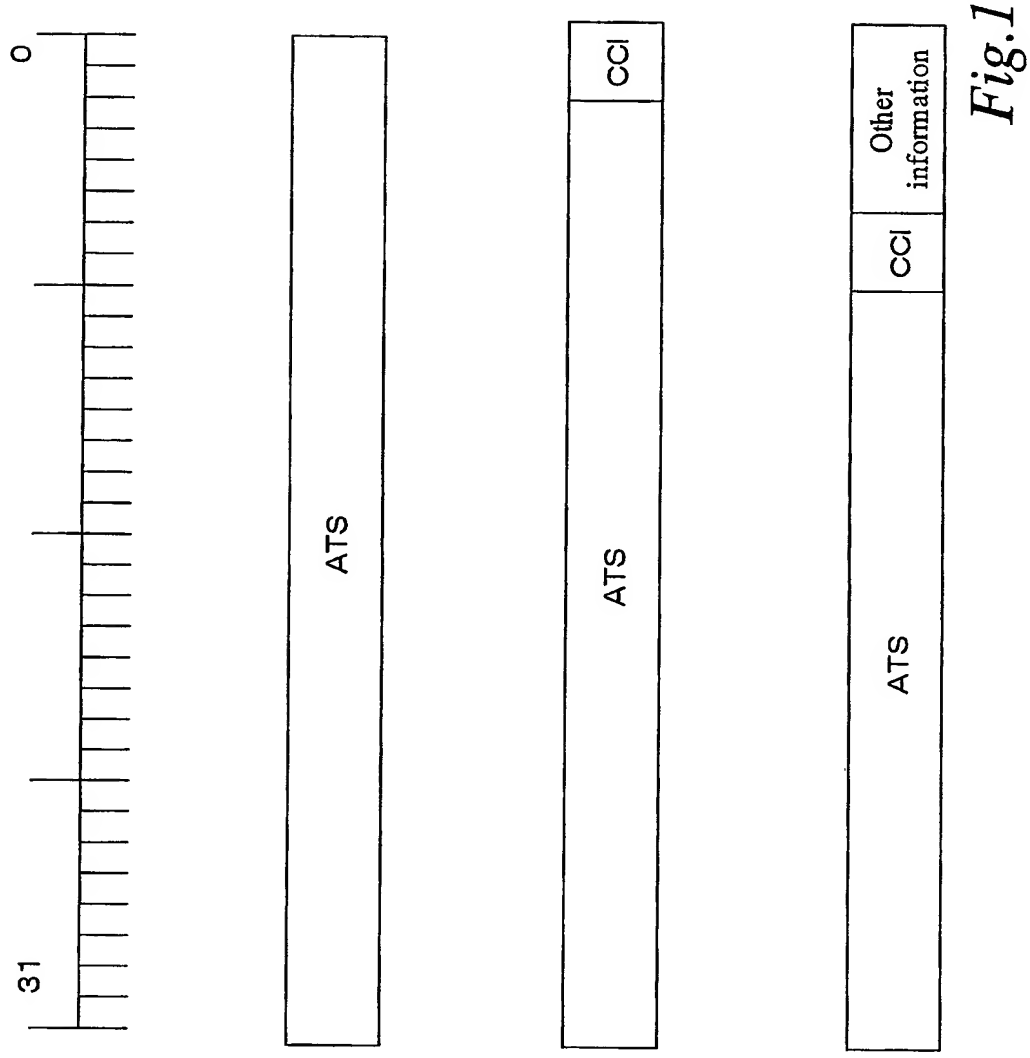

入力ビデオ
901
MPEG ビデオ エンコーダ
902
ビデオ ストリーム バッファ
903
入力 オーディオ
904
MPEG オーディオ エンコーダ
905
オーディオ ストリーム バッファ
906
アクセスユニット 情報
多重化 スケジューラ
908
パケット符号化制御情報
トランスポート パケット 符号化器
909
ブロックシード (Block seed) 付加回路
911
スムージング バッファ
912
913
記録AVデータ
(暗号処理手段を介して記録媒体へ入力)
到着(Arrival) タイムスタンプ 計算手段
910
ATS
976
a
b

Fig.9



ブロックシード (Block Seed)

例1
ATS 32bit

例2
ATS 30bit
CCI 2bit

例3
ATS 24bit
CCI 2bit
other info 6bit

Fig.10

入力ソース	アナログ出力		デジタル出力	備考
	水平解像度	コピー保護 (Macrovision 等)		
5C	600 本以下	要	5C 相当以上	Copy Free のコンテンツに関してはすべて制限なし
BS, CS	800 本以下	不要	禁止	
地上波デジタル	制限なし	要	5C 相当以上	
地上波アナログ	制限なし	不要	禁止	
その他	制限なし	不要	制限なし	

Fig.11

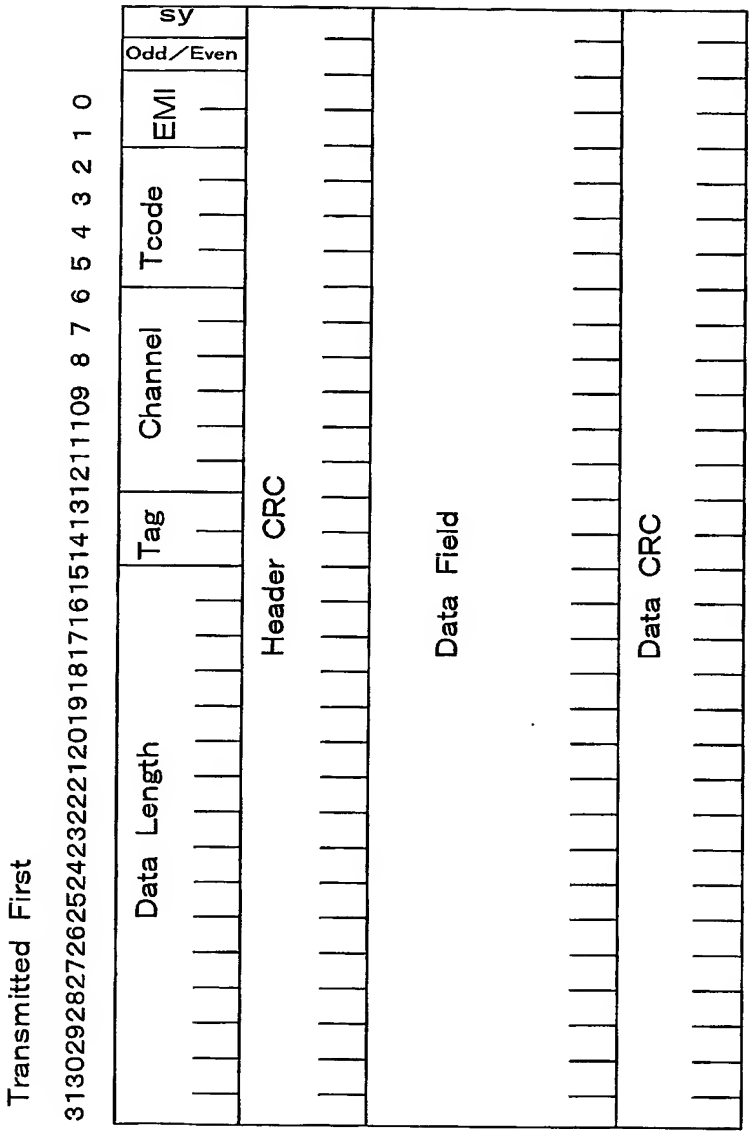
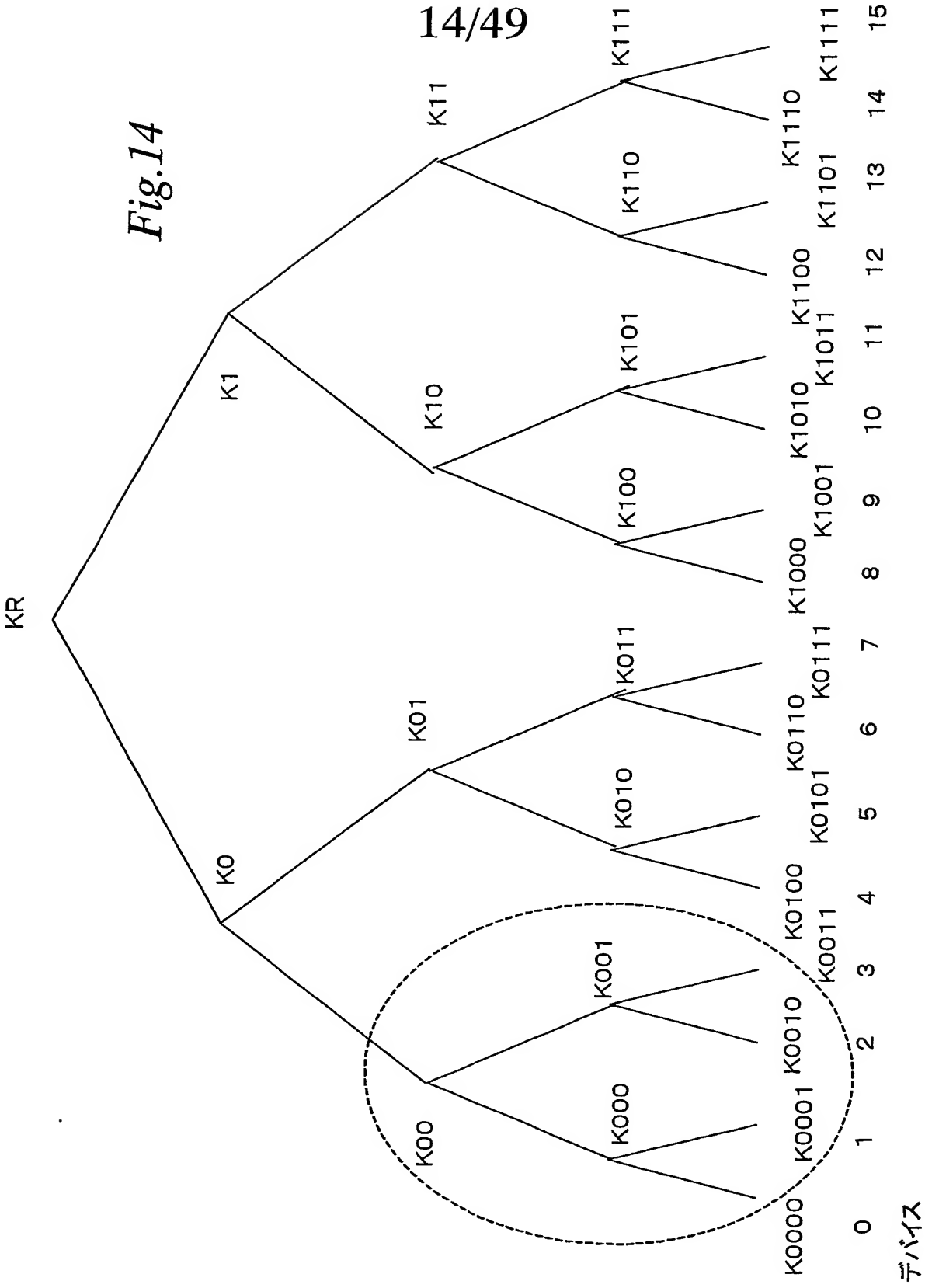

Transmitted First
31302928272625242322212019181716151413121110 9 8 7 6 5 4 3 2 1 0
Data Length
Tag
Channel
Tcode
EMI
Odd/Even
sy
Header CRC
Data Field
Data CRC

Fig.12

コピー制御情報(2bit)	変化点(TSパケットNo.)(30bit)
00(Copy Free)	0
10(No More Copy)	300000(0x00007530)
00(Copy Free)	100000(0x000186A0)
10(No More Copy)	1234567(0x0012D687)

Fig.13

Fig.14


KR
K0
K1
K00
K01
K10
K11
K000
K001
K010
K011
K100
K101
K110
K111
K0000
K0001
K0010
K0011
K0100
K0101
K0110
K0111
K1000
K1001
K1010
K1011
K1100
K1101
K1110
K1111
0
1
2
3
4
5
6
7
8
9
10
11
12
13
14
15
デバイス

(A) キー更新ブロック(KRB:Key Renewal Block) 例1

デバイス0, 1, 2にt時点でのルートキーK(t)Rを送付

世代(Generztion):t	
インデックス	暗号化キー
0	Enc(K(t)0, K(t)R)
00	Enc(K(t)00, K(t)0)
000	Enc(K000, K(t)00)
001	Enc(K(t)001, K(t)00)
0010	Enc(K0010, K(t)001)

(B) キー更新ブロック(KRB:Key Renewal Block) 例2

デバイス0, 1, 2にt時点でのルートキーK(t)Rを送付

世代(Generztion):t	
インデックス	暗号化キー
000	Enc(K000, K(t)00)
001	Enc(K(t)001, K(t)00)
0010	Enc(K0010, K(t)001)

Fig.15

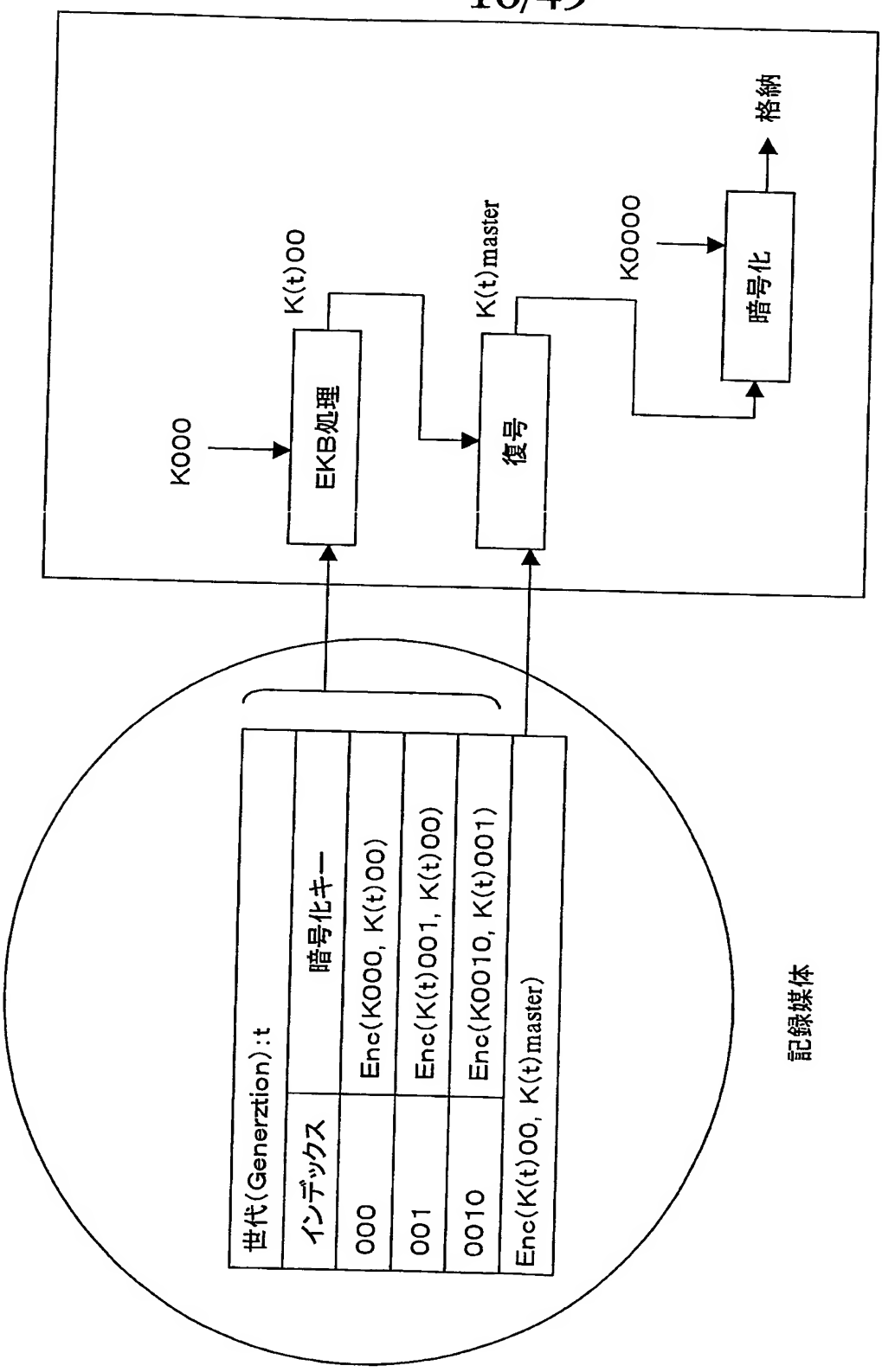

K000
EKB処理
K(t)00
復号
K(t)master
K0000
暗号化
格納
デバイス0
記録媒体
世代(Generztion):t
インデックス
暗号化キー
000
Enc(K000, K(t)00)
001
Enc(K(t)001, K(t)00)
0010
Enc(K0010, K(t)001)
Enc(K(t)00, K(t)master)

Fig.16

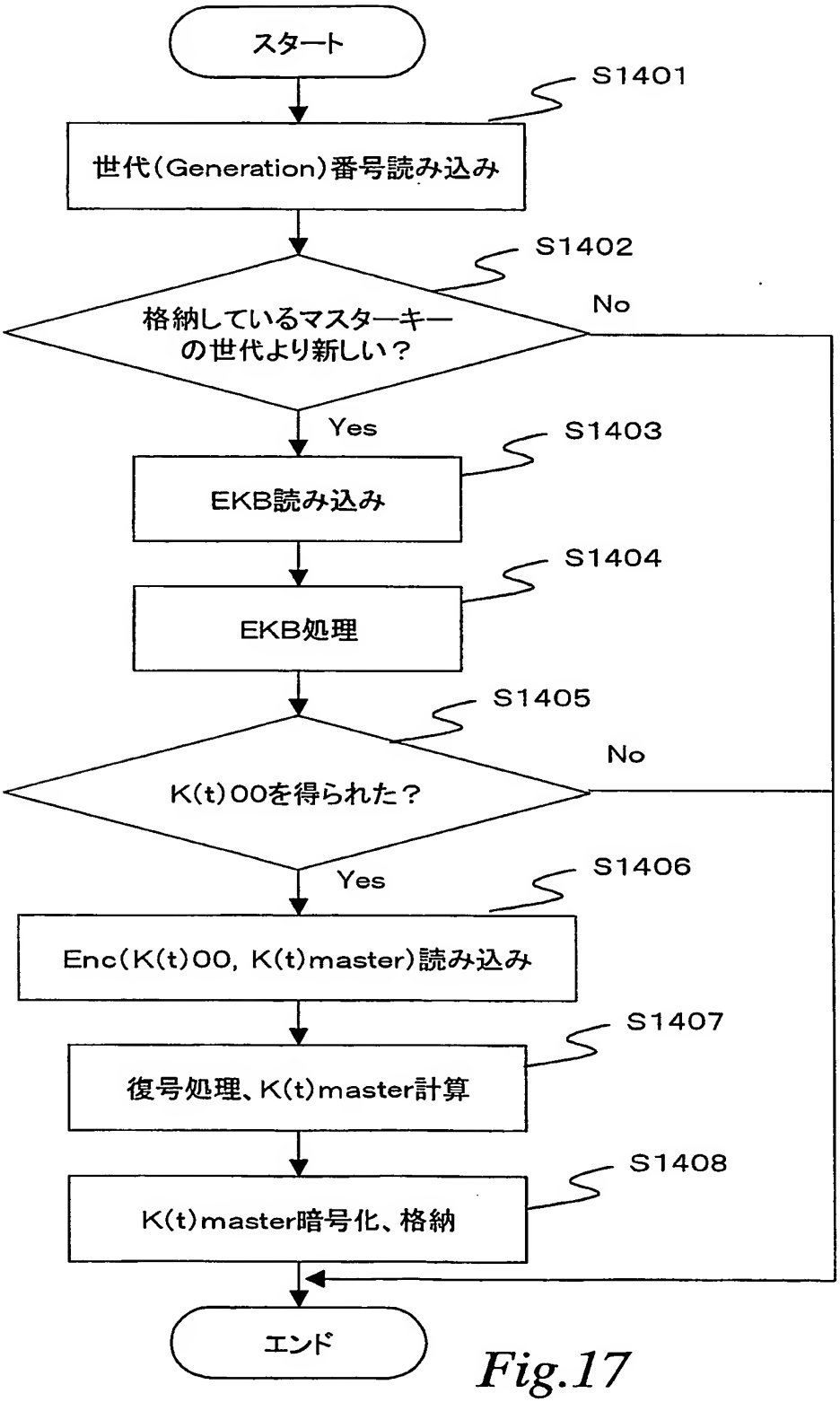

スタート
S1401
世代(Generation)番号読み込み
S1402
格納しているマスターキーの世代より新しい？
No
Yes
S1403
EKB読み込み
S1404
EKB処理
S1405
K(t)00を得られた？
No
Yes
S1406
Enc(K(t)00, K(t)master)読み込み
S1407
復号処理、K(t)master計算
S1408
K(t)master暗号化、格納
エンド

Fig.17

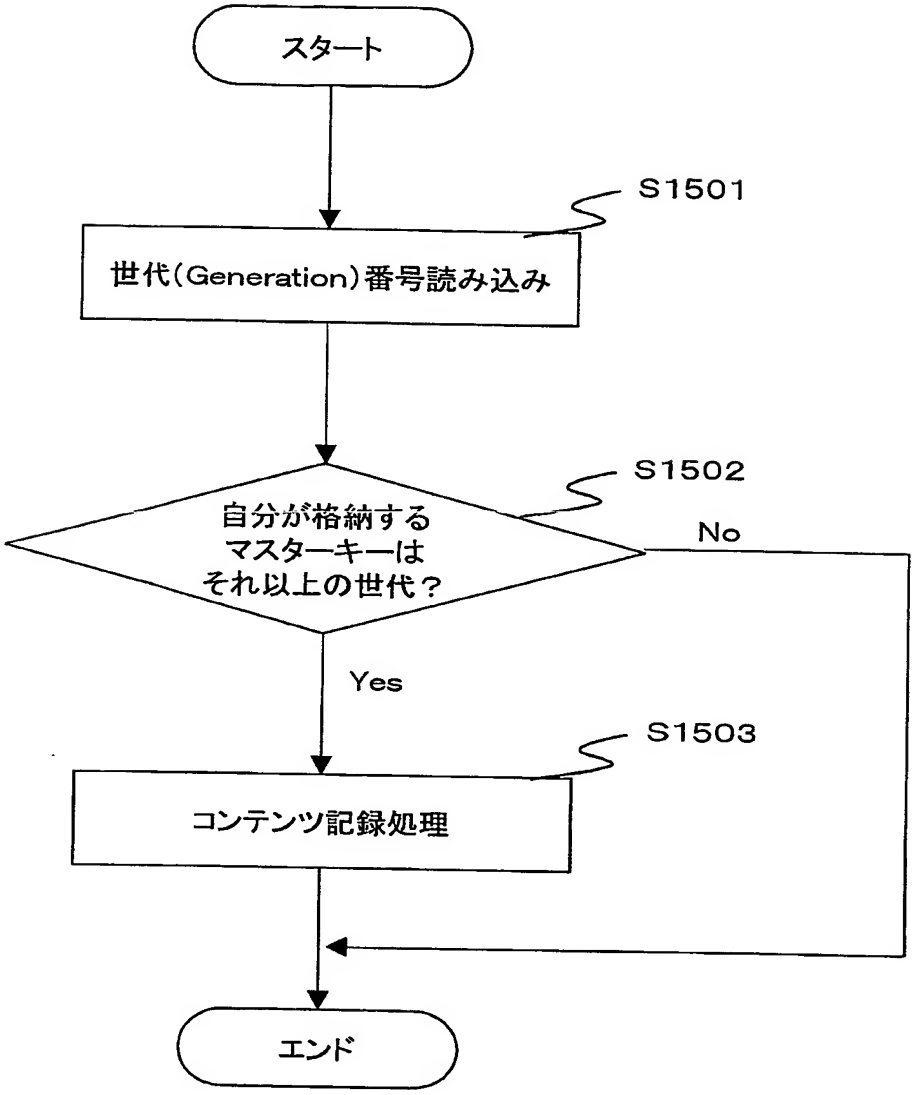

スタート
S1501
世代(Generation)番号読み込み
S1502
自分が格納する
マスターキーは
それ以上の世代？
No
Yes
S1503
コンテンツ記録処理
エンド

Fig.18

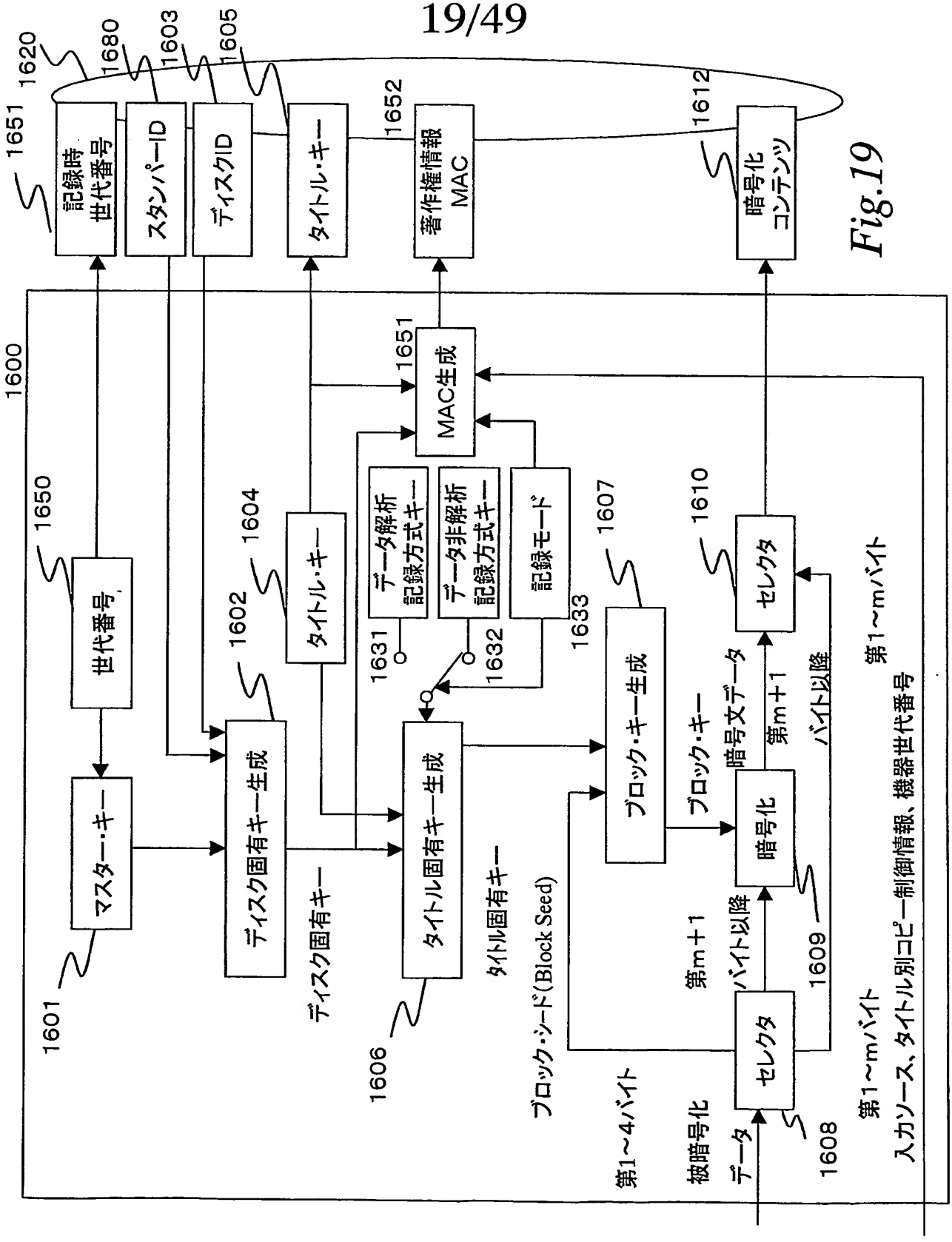

1620
1680
1603
1605
1651
記録時 世代番号
スタンパーID
ディスクID
タイトル・キー
1652
著作権情報 MAC
1612
暗号化 コンテンツ
1600
1650
世代番号
1651
MAC生成
1604
タイトル・キー
データ解析 記録方式キー
データ非解析 記録方式キー
記録モード
1607
1610
セレクタ
1602
1631
1632
1633
ブロック・キー生成
マスター・キー
ディスク固有キー生成
タイトル固有キー生成
ブロック・キー
暗号文データ
暗号化
第m＋1 バイト以降
第m＋1 バイト以降
1601
ディスク固有キー
1606
タイトル固有キー
ブロック・シード(Block Seed)
1609
第1～mバイト
第1～4バイト
被暗号化 データ
セレクタ
1608
第1～mバイト
入力ソース、タイトル別コピー制御情報、機器世代番号

Fig.19

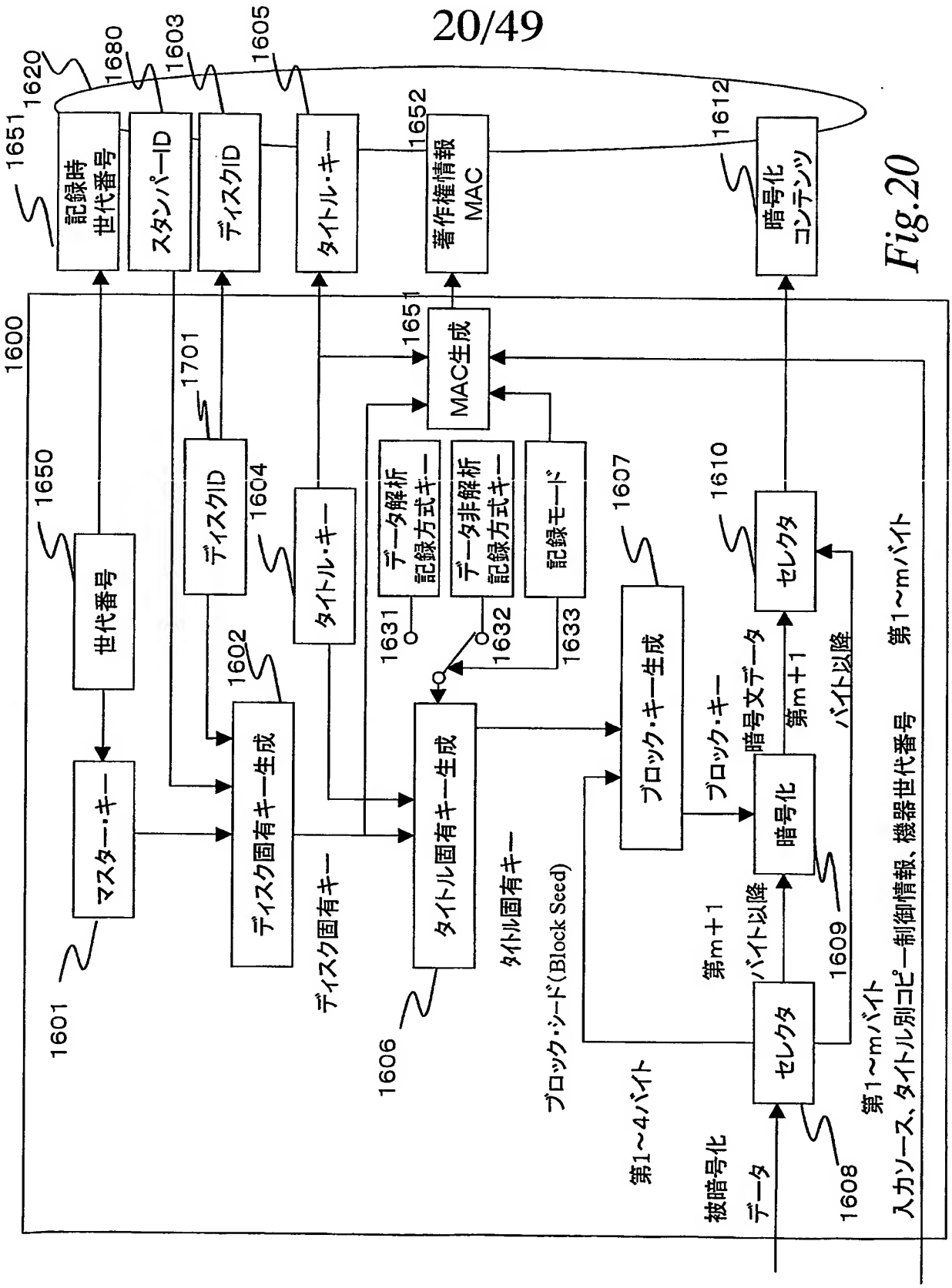

1600
1601
マスター・キー
1602
ディスク固有キー生成
ディスク固有キー
1603
スタンパーID
1604
ディスクID
1605
タイトル・キー
1606
タイトル固有キー生成
タイトル固有キー
1607
ブロック・キー生成
ブロック・シード(Block Seed)
第1～4バイト
1608
セレクタ
被暗号化データ
1609
暗号化
第m＋1バイト以降
1610
セレクタ
第m＋1バイト以降
暗号文データ
第1～mバイト
1612
暗号化コンテンツ
1620
1631
データ解析記録方式キー
1632
データ非解析記録方式キー
1633
記録モード
1650
世代番号
1651
記録時世代番号
1652
著作権情報MAC
1680
1701
ディスクID
MAC生成
入力ソース、タイトル別コピー制御情報、機器世代番号
第1～mバイト

Fig.20

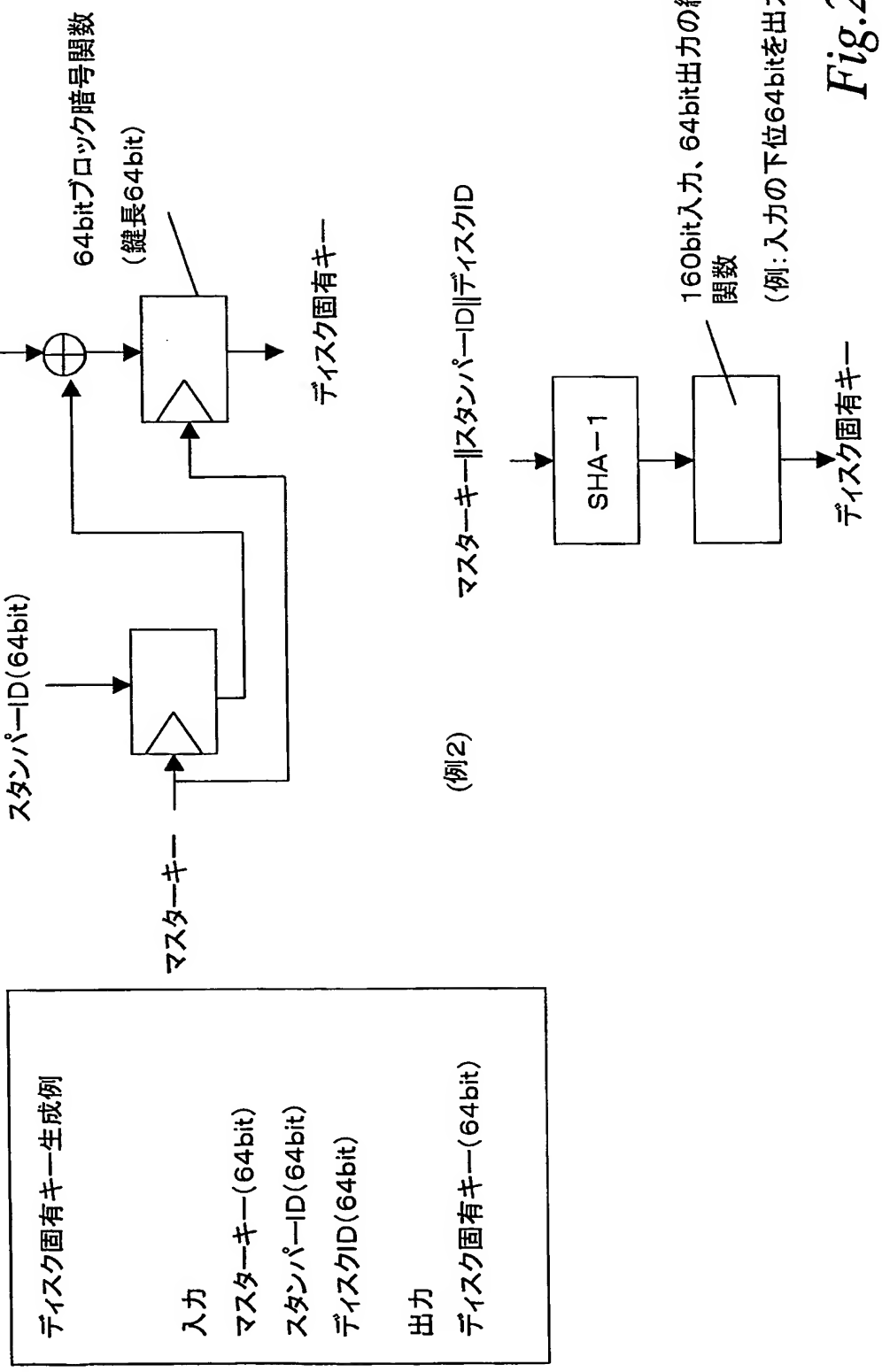

ディスク固有キー生成例
入力
マスターキー(64bit)
スタンパーID(64bit)
ディスクID(64bit)
出力
ディスク固有キー(64bit)
マスターキー
スタンパーID(64bit)
(例1)
ディスクID(64bit)
64bitブロック暗号関数
(鍵長64bit)
ディスク固有キー
(例2)
マスターキー||スタンパーID||ディスクID
SHA-1
160bit入力、64bit出力の縮約関数
(例:入力の下位64bitを出力)
ディスク固有キー

Fig.21

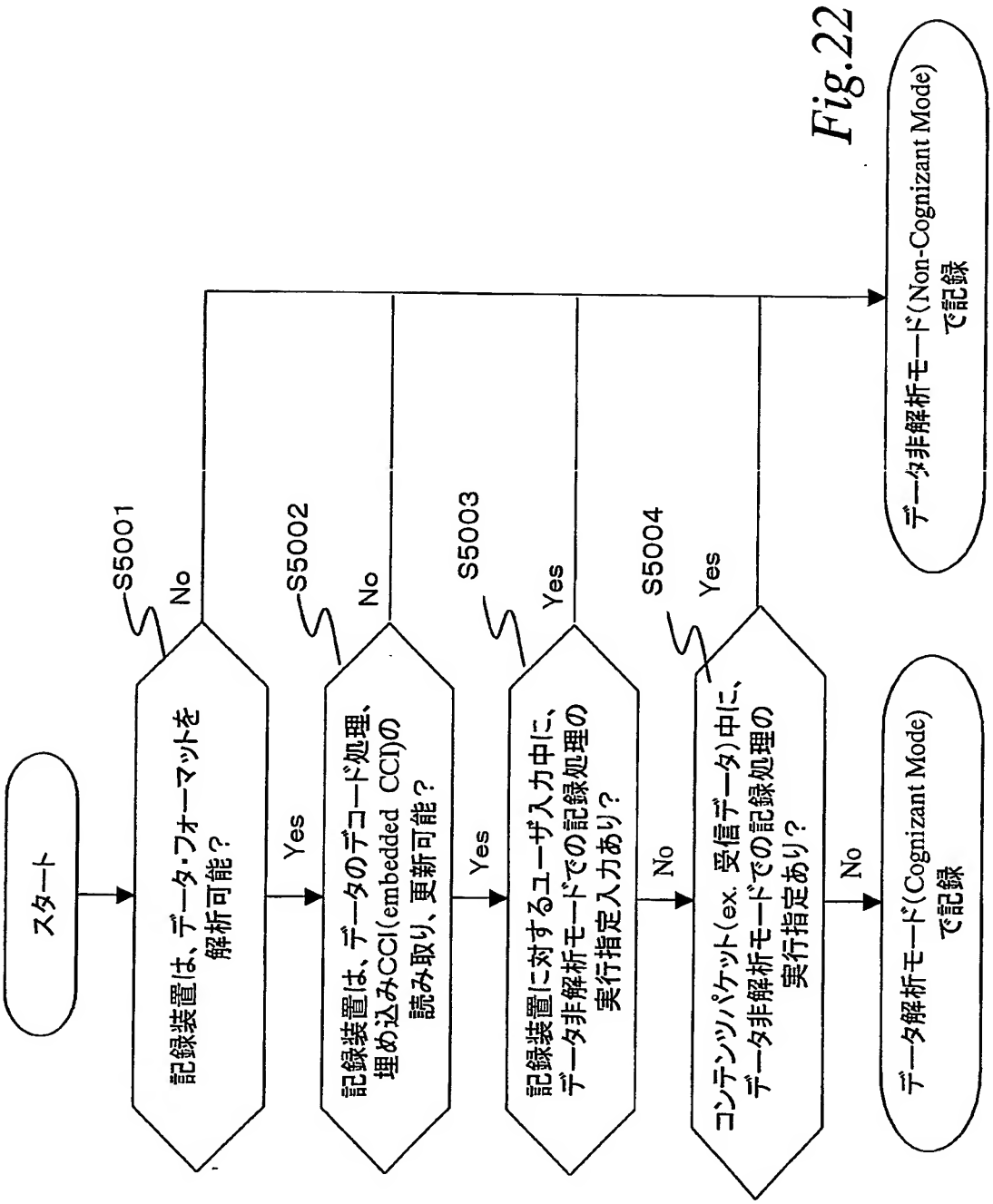

スタート
S5001
記録装置は、データ・フォーマットを解析可能？
No
Yes
S5002
記録装置は、データのデコード処理、埋め込みCCI(embedded CCI)の読み取り、更新可能？
No
Yes
S5003
記録装置に対するユーザ入力中に、データ非解析モードでの記録処理の実行指定入力あり？
Yes
No
S5004
コンテンツパケット(ex. 受信データ)中に、データ非解析モードでの記録処理の実行指定あり？
No
Yes
データ解析モード(Cognizant Mode)で記録
データ非解析モード(Non-Cognizant Mode)で記録

Fig.22

タイトル固有キー生成例

入力

ディスク固有キー(64bit)

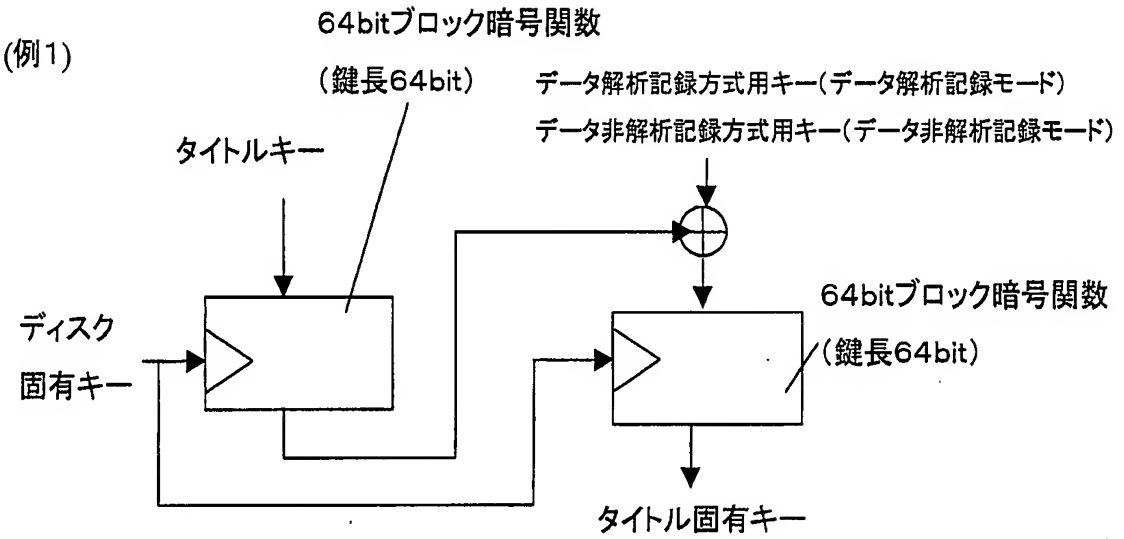
タイトルキー(64bit)

データ解析記録方式用キー(64bit)、またはデータ非解析記録方式用キー(64bit)

出力

タイトル固有キー(64bit)

(例1)



(例2)

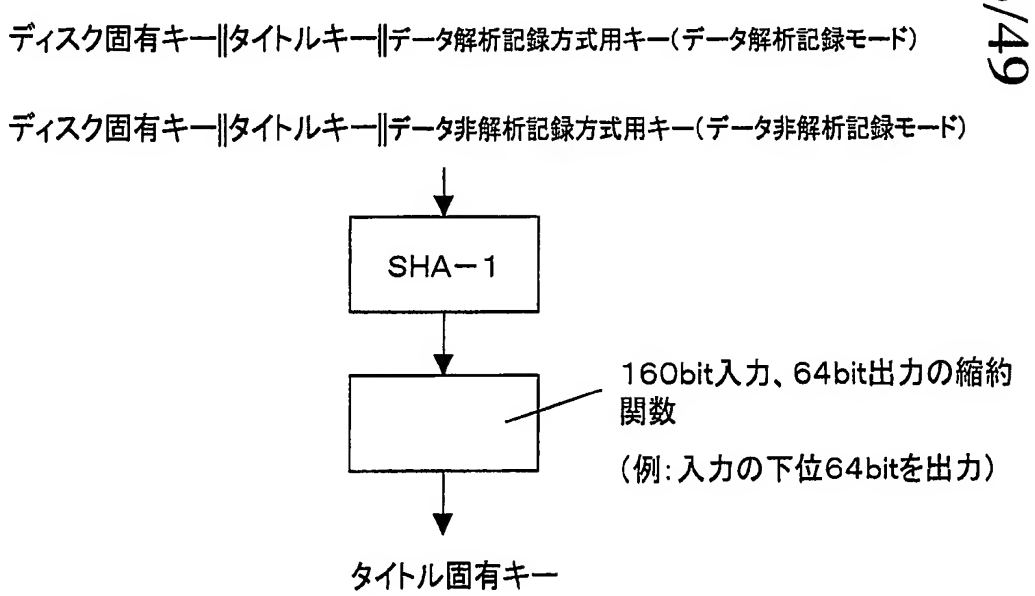
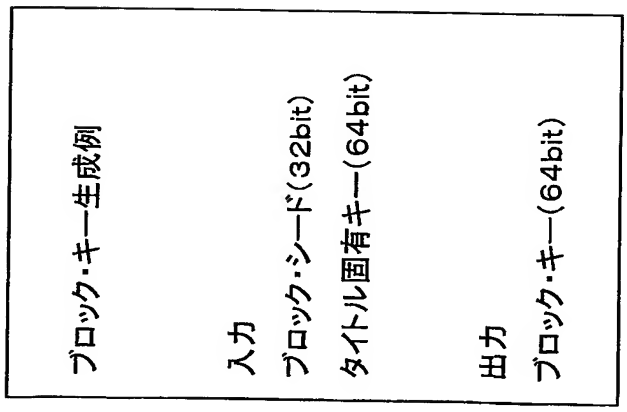


Fig.23


ブロック・キー生成例
入力
ブロック・シード(32bit)
タイトル固有キー(64bit)
出力
ブロック・キー(64bit)

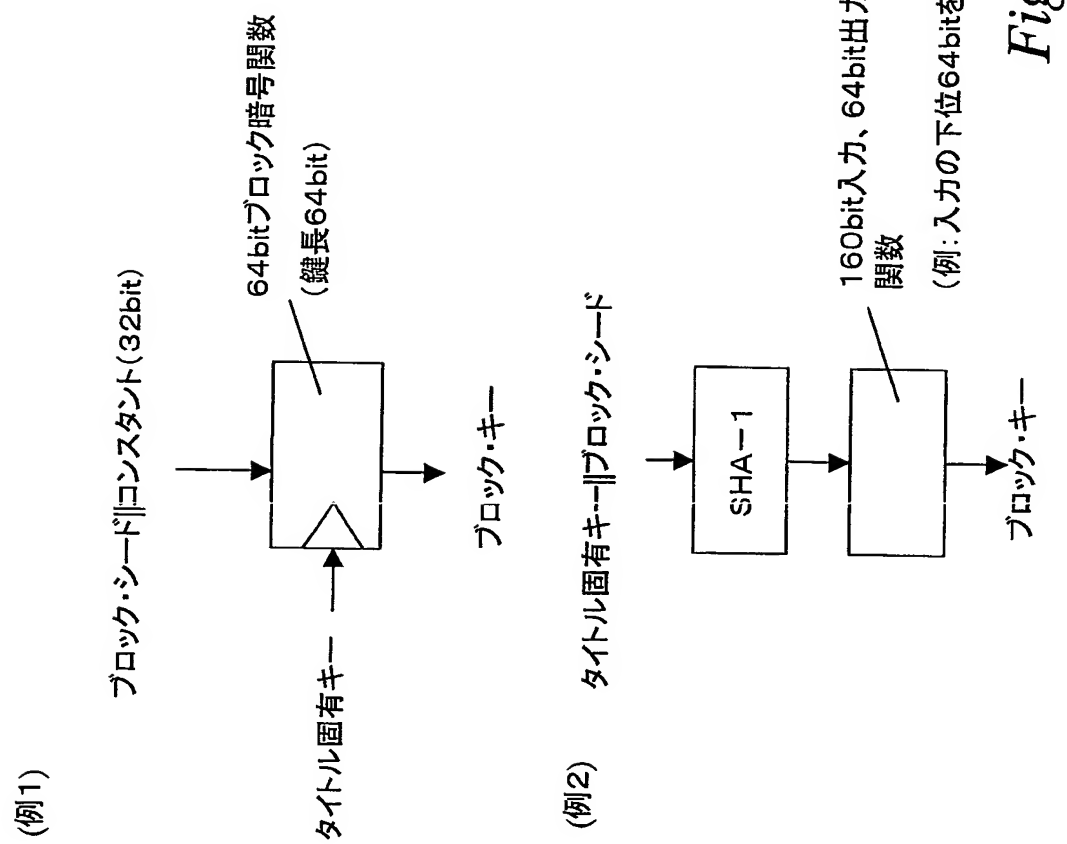

(例1)
ブロック・シード‖コンスタント(32bit)
64bitブロック暗号関数
(鍵長64bit)
タイトル固有キー
ブロック・キー
(例2)
タイトル固有キー‖ブロック・シード
SHA−1
160bit入力、64bit出力の縮約関数
(例:入力の下位64bitを出力)
ブロック・キー

Fig.24

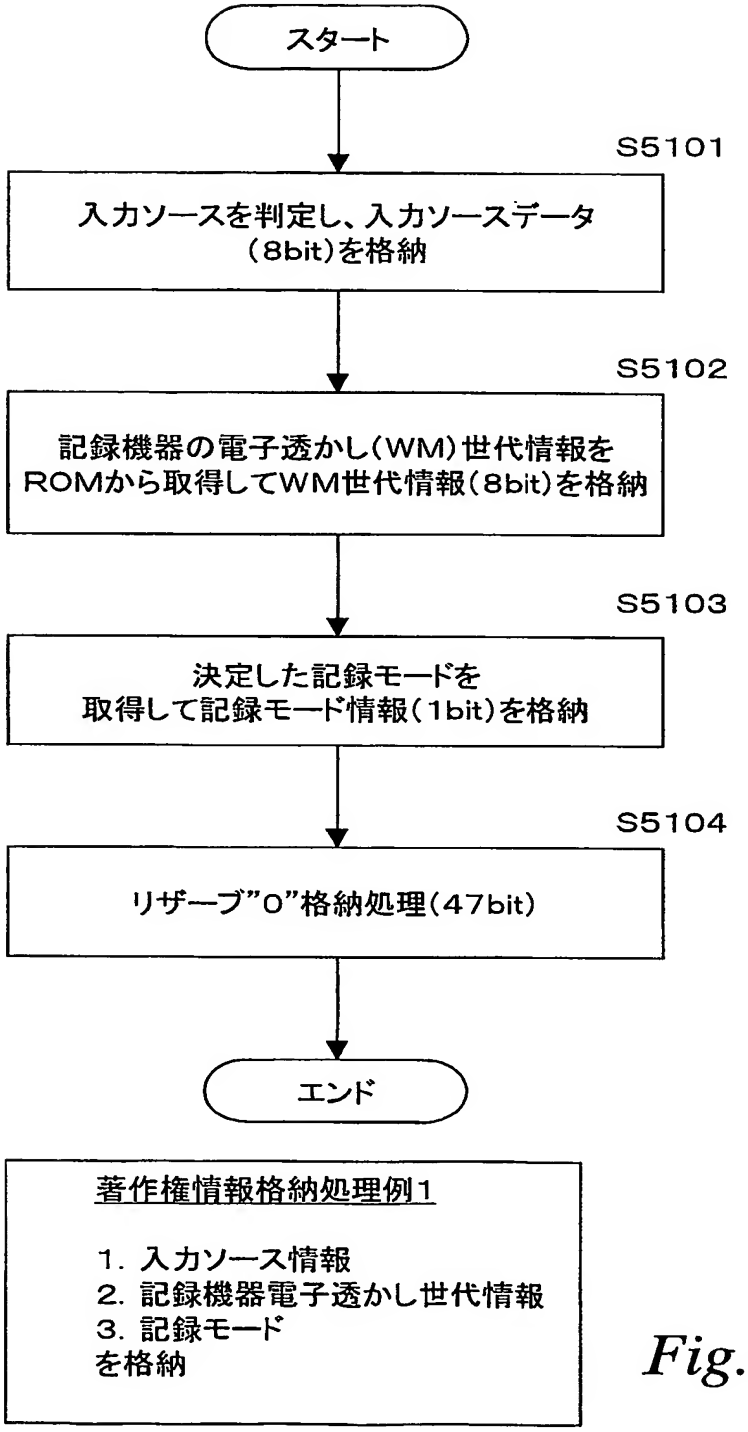

スタート
S5101
入力ソースを判定し、入力ソースデータ
(8bit)を格納
S5102
記録機器の電子透かし(WM)世代情報を
ROMから取得してWM世代情報(8bit)を格納
S5103
決定した記録モードを
取得して記録モード情報(1bit)を格納
S5104
リザーブ"0"格納処理(47bit)
エンド
著作権情報格納処理例1
1. 入力ソース情報
2. 記録機器電子透かし世代情報
3. 記録モード
を格納

Fig.25

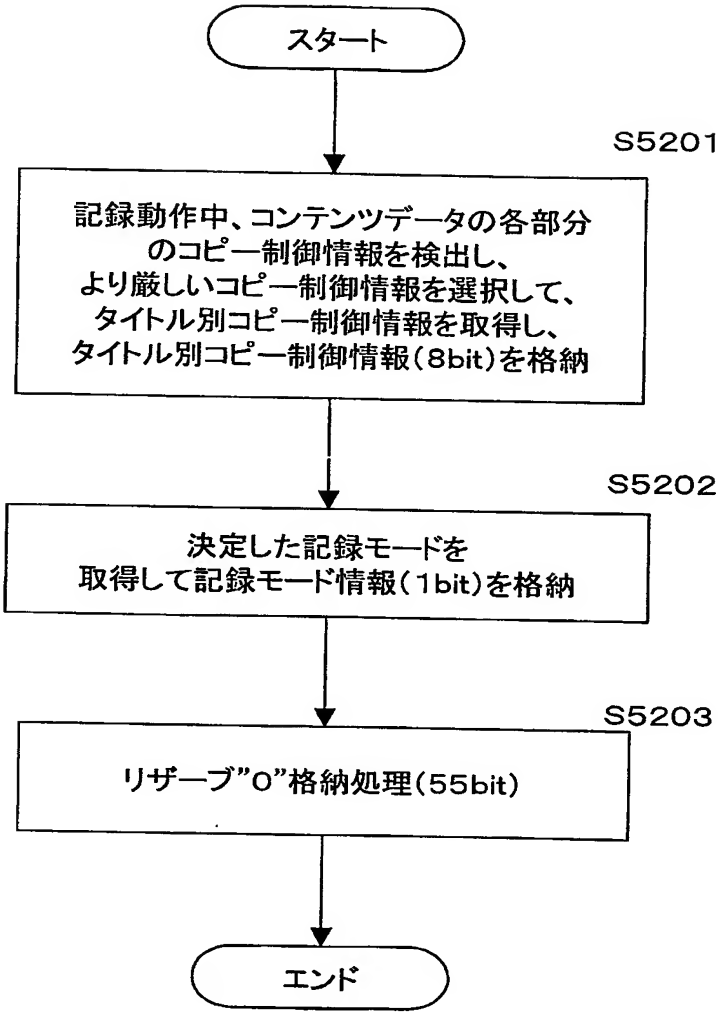
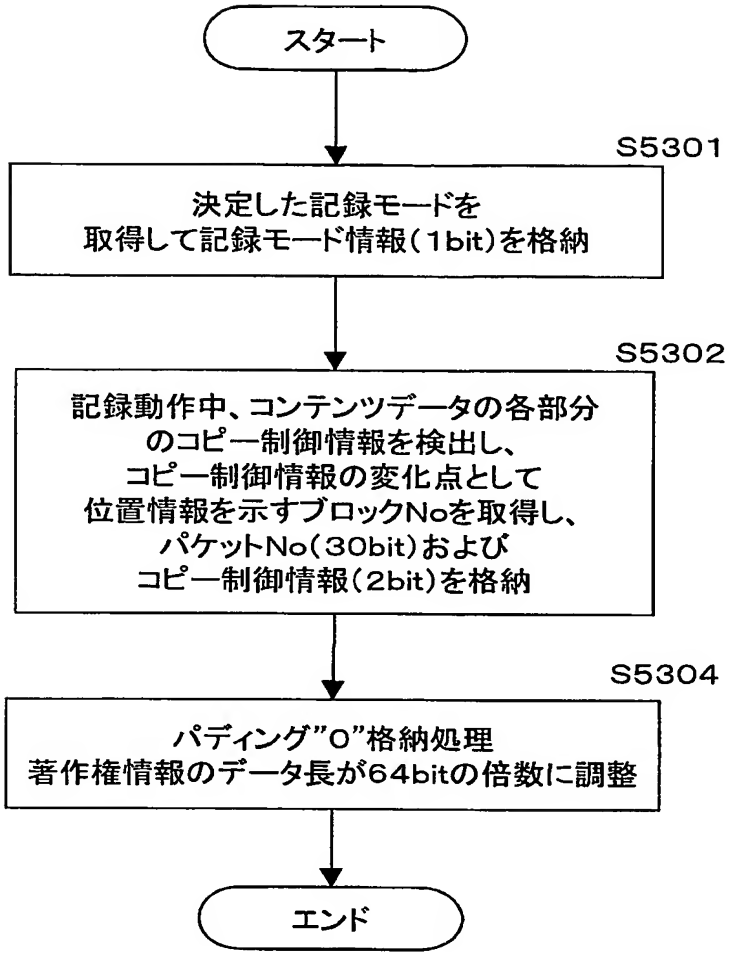

スタート
S5201
記録動作中、コンテンツデータの各部分
のコピー制御情報を検出し、
より厳しいコピー制御情報を選択して、
タイトル別コピー制御情報を取得し、
タイトル別コピー制御情報(8bit)を格納
S5202
決定した記録モードを
取得して記録モード情報(1bit)を格納
S5203
リザーブ"0"格納処理(55bit)
エンド
著作権情報格納処理例2
1. タイトル別コピー制御情報
2. 記録モード
を格納

Fig.26



著作権情報格納処理例3

1. 記録モード
2. コピー制御情報の変化点情報
を格納

Fig.27

著作権情報MAC生成例

入力

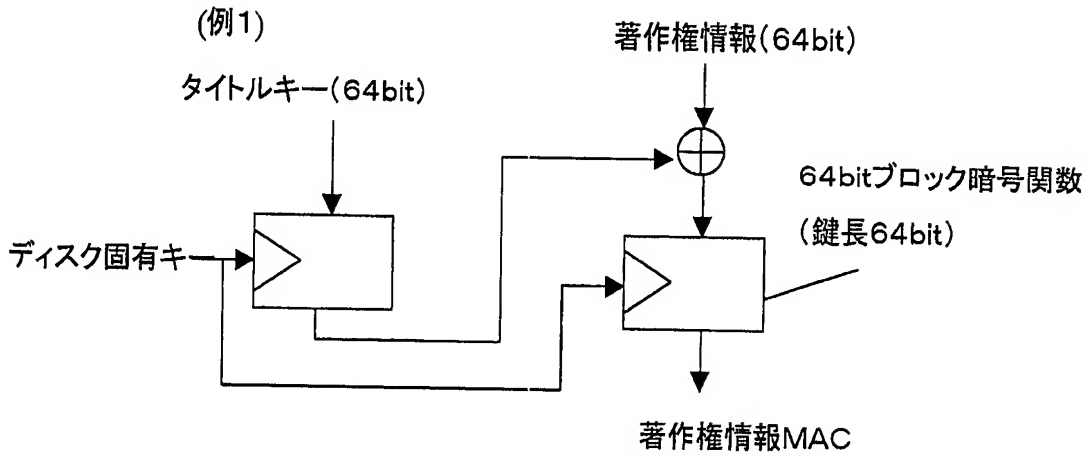
ディスク固有キー(64bit)

タイトルキー(64bit)

著作権情報(64bit)

出力

著作権情報MAC(64bit)



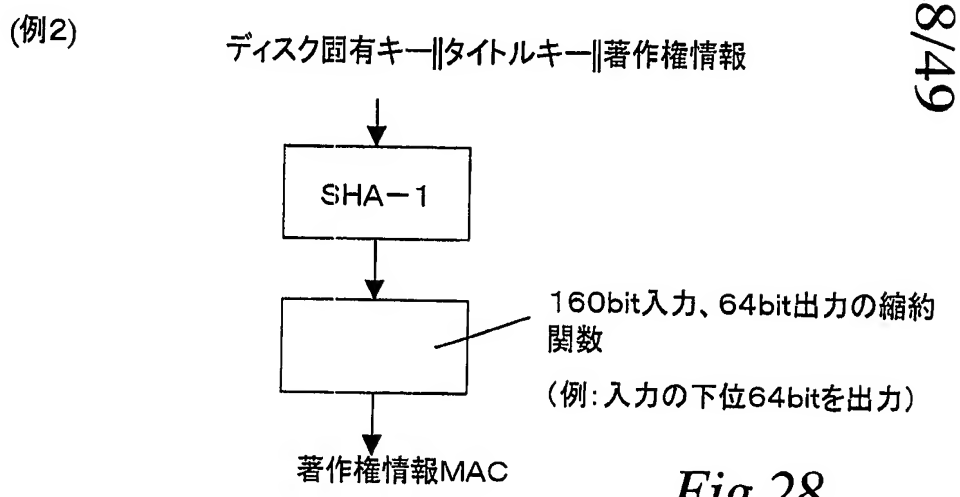


Fig.28

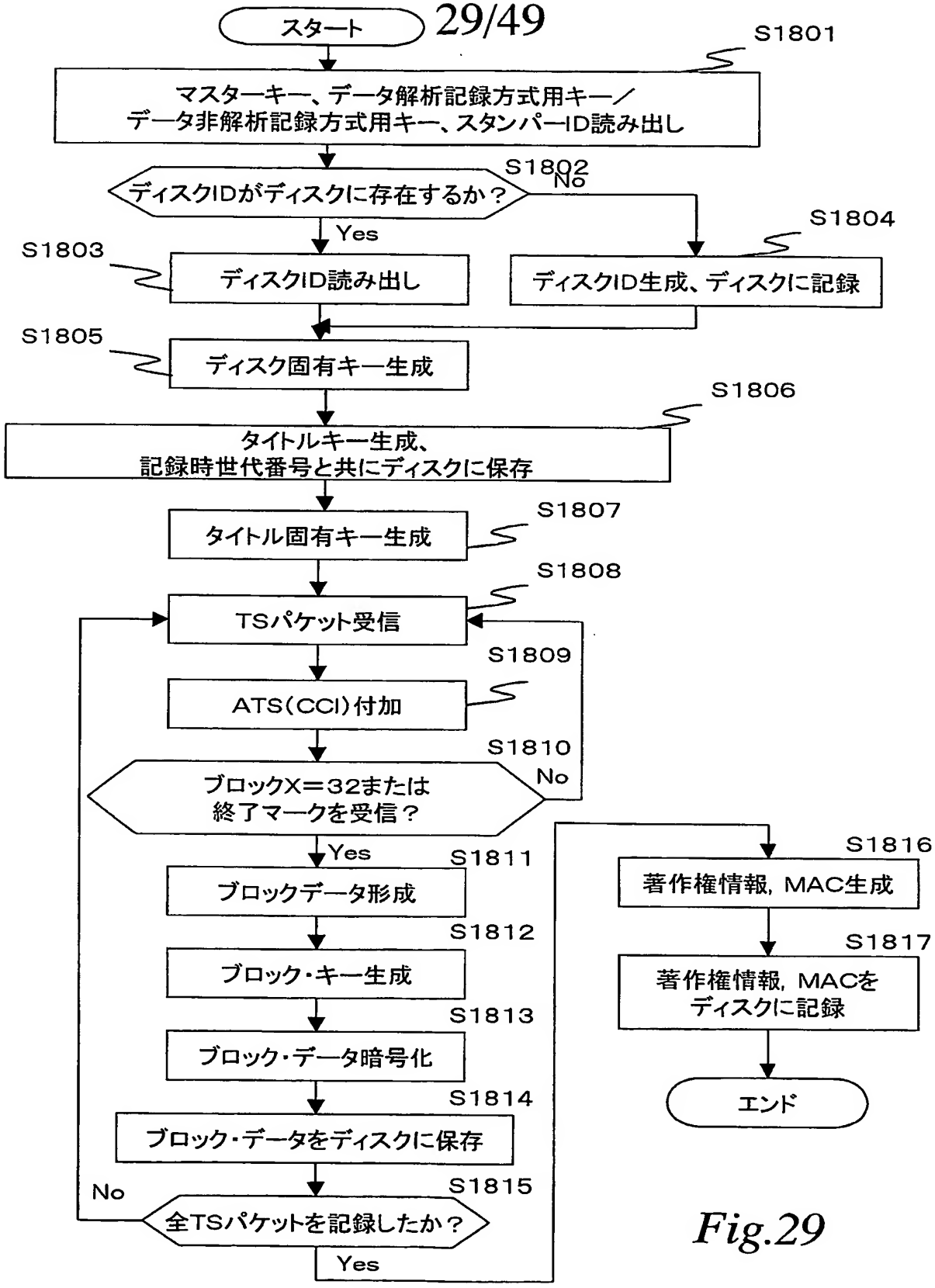

スタート
S1801
マスターキー、データ解析記録方式用キー／
データ非解析記録方式用キー、スタンパーID読み出し
S1802
ディスクIDがディスクに存在するか？
No
Yes
S1803
ディスクID読み出し
S1804
ディスクID生成、ディスクに記録
S1805
ディスク固有キー生成
S1806
タイトルキー生成、
記録時世代番号と共にディスクに保存
S1807
タイトル固有キー生成
S1808
TSパケット受信
S1809
ATS(CCI)付加
S1810
ブロックX＝32または
終了マークを受信？
No
Yes
S1811
ブロックデータ形成
S1812
ブロック・キー生成
S1813
ブロック・データ暗号化
S1814
ブロック・データをディスクに保存
S1815
No
全TSパケットを記録したか？
Yes
S1816
著作権情報，MAC生成
S1817
著作権情報，MACを
ディスクに記録
エンド

Fig.29

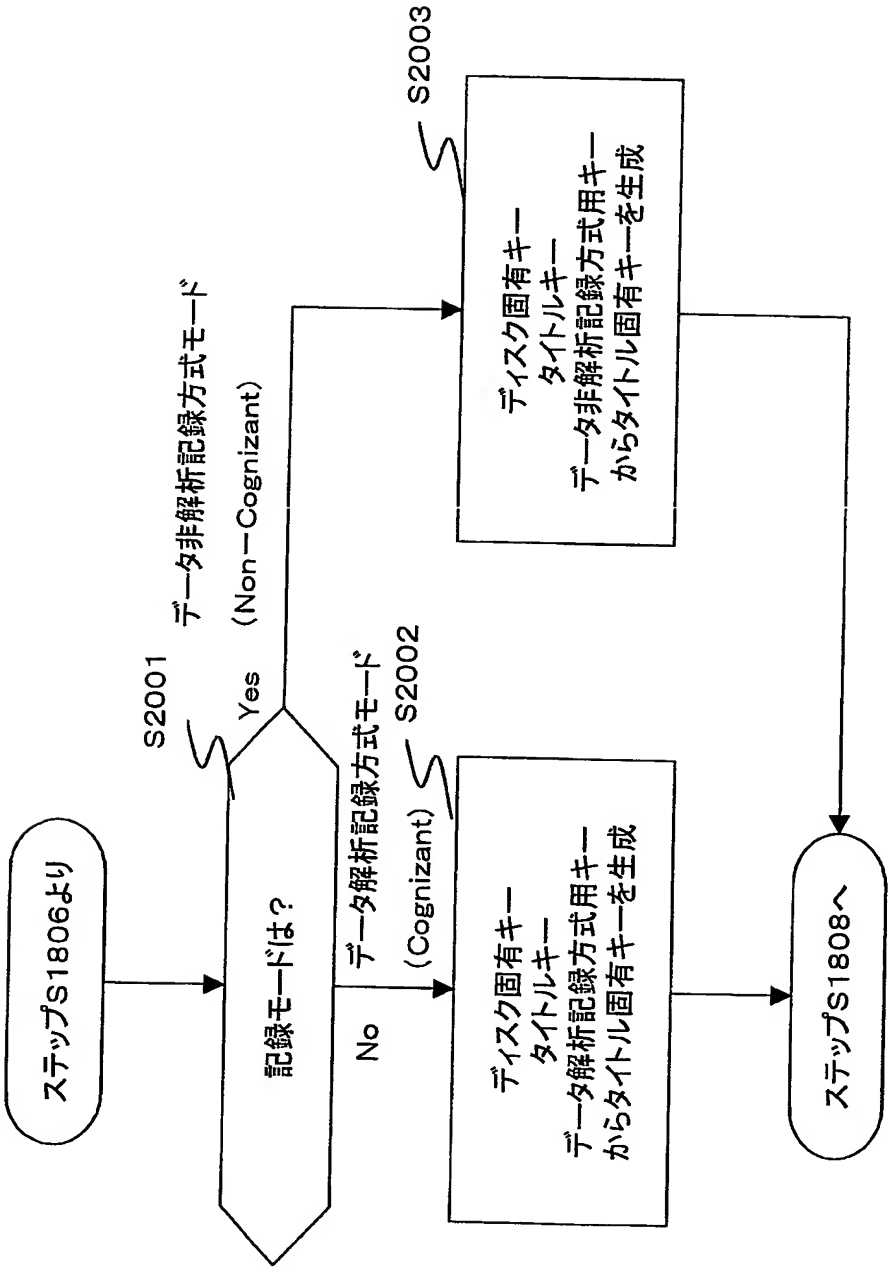

ステップS1806より
記録モードは？
S2001
データ非解析記録方式モード
(Non−Cognizant)
Yes
No
データ解析記録方式モード
S2002
(Cognizant)
S2003
ディスク固有キー
タイトルキー
データ非解析記録方式用キー
からタイトル固有キーを生成
ディスク固有キー
タイトルキー
データ解析記録方式用キー
からタイトル固有キーを生成
ステップS1808へ

Fig.30

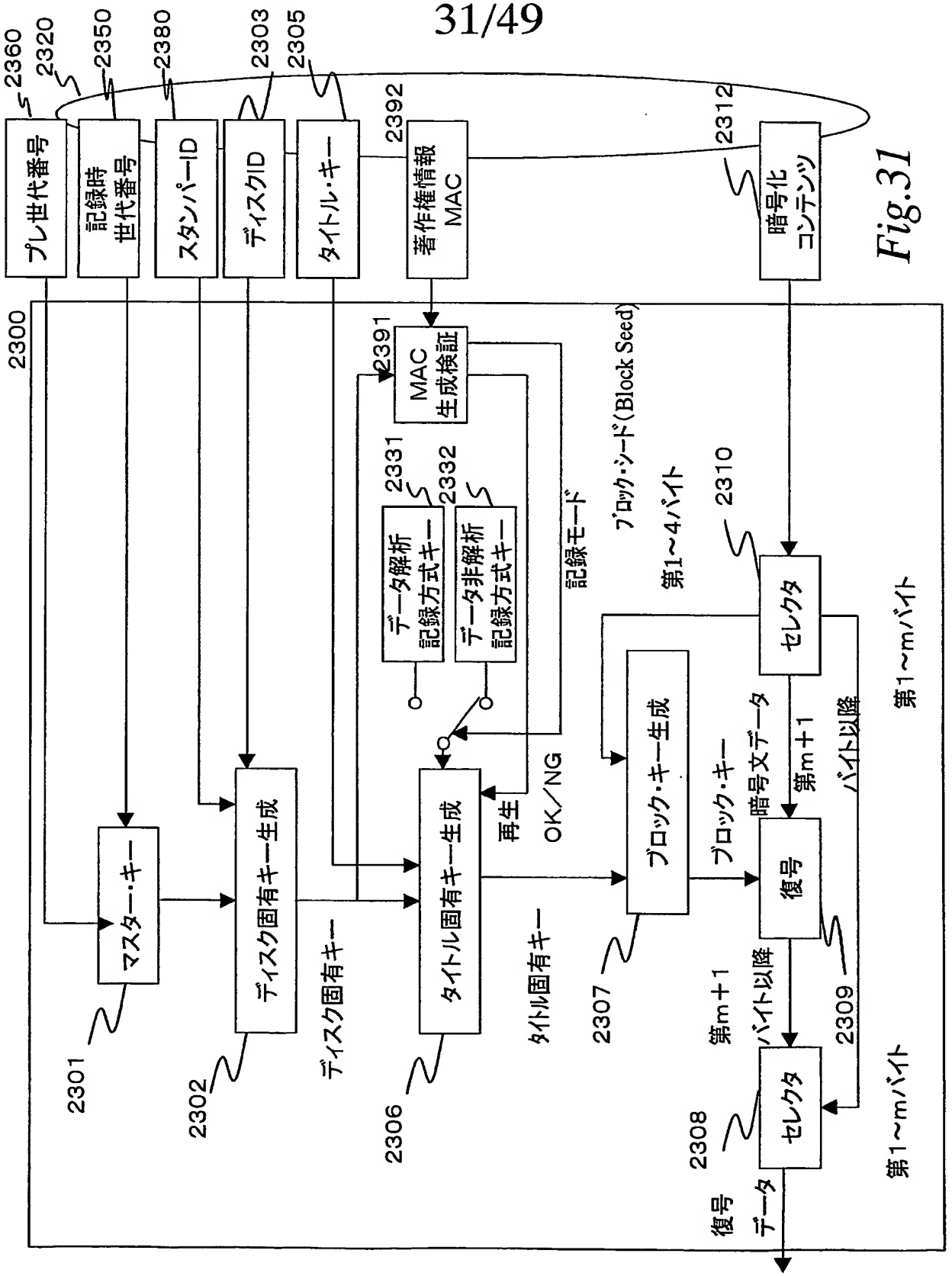

2360
2320
2350
2380
2303
2305
2392
2312
プレ世代番号
記録時世代番号
スタンパーID
ディスクID
タイトル・キー
著作権情報MAC
暗号化コンテンツ
2300
2391
MAC生成検証
2331
2332
データ解析記録方式キー
データ非解析記録方式キー
記録モード
ブロック・シード(Block Seed)
第1～4バイト
2310
セレクタ
第1～mバイト
マスター・キー
ディスク固有キー生成
タイトル固有キー生成
再生
OK／NG
ブロック・キー生成
ブロック・キー
暗号文データ
第m＋1
バイト以降
復号
2301
2302
ディスク固有キー
2306
タイトル固有キー
2307
第m＋1
バイト以降
2309
2308
セレクタ
第1～mバイト
復号データ

Fig.31

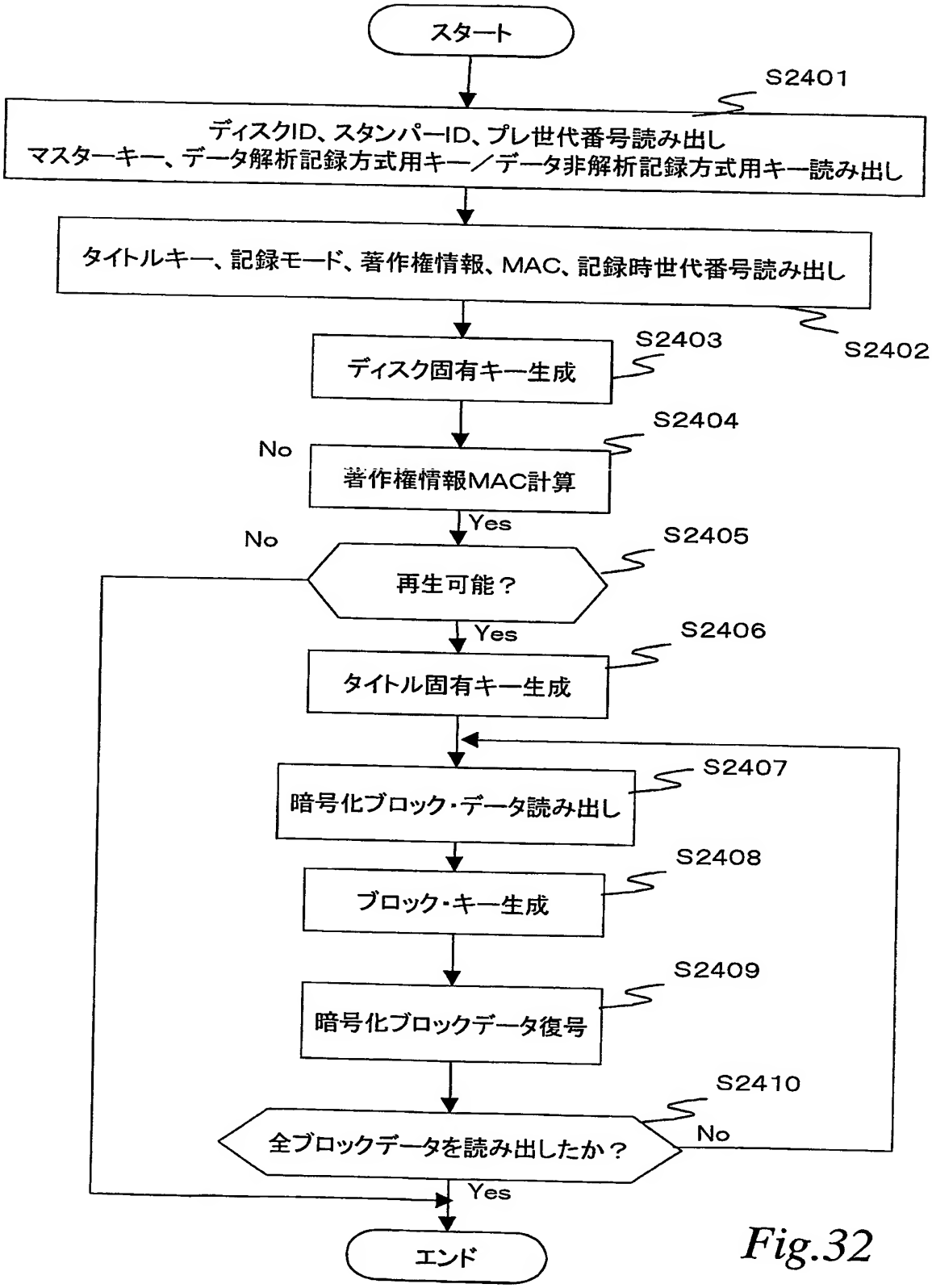

スタート
S2401
ディスクID、スタンパーID、プレ世代番号読み出し
マスターキー、データ解析記録方式用キー／データ非解析記録方式用キー読み出し
タイトルキー、記録モード、著作権情報、MAC、記録時世代番号読み出し
S2402
ディスク固有キー生成
S2403
No
著作権情報MAC計算
S2404
Yes
No
再生可能？
S2405
Yes
タイトル固有キー生成
S2406
暗号化ブロック・データ読み出し
S2407
ブロック・キー生成
S2408
暗号化ブロックデータ復号
S2409
全ブロックデータを読み出したか？
S2410
No
Yes
エンド

Fig.32

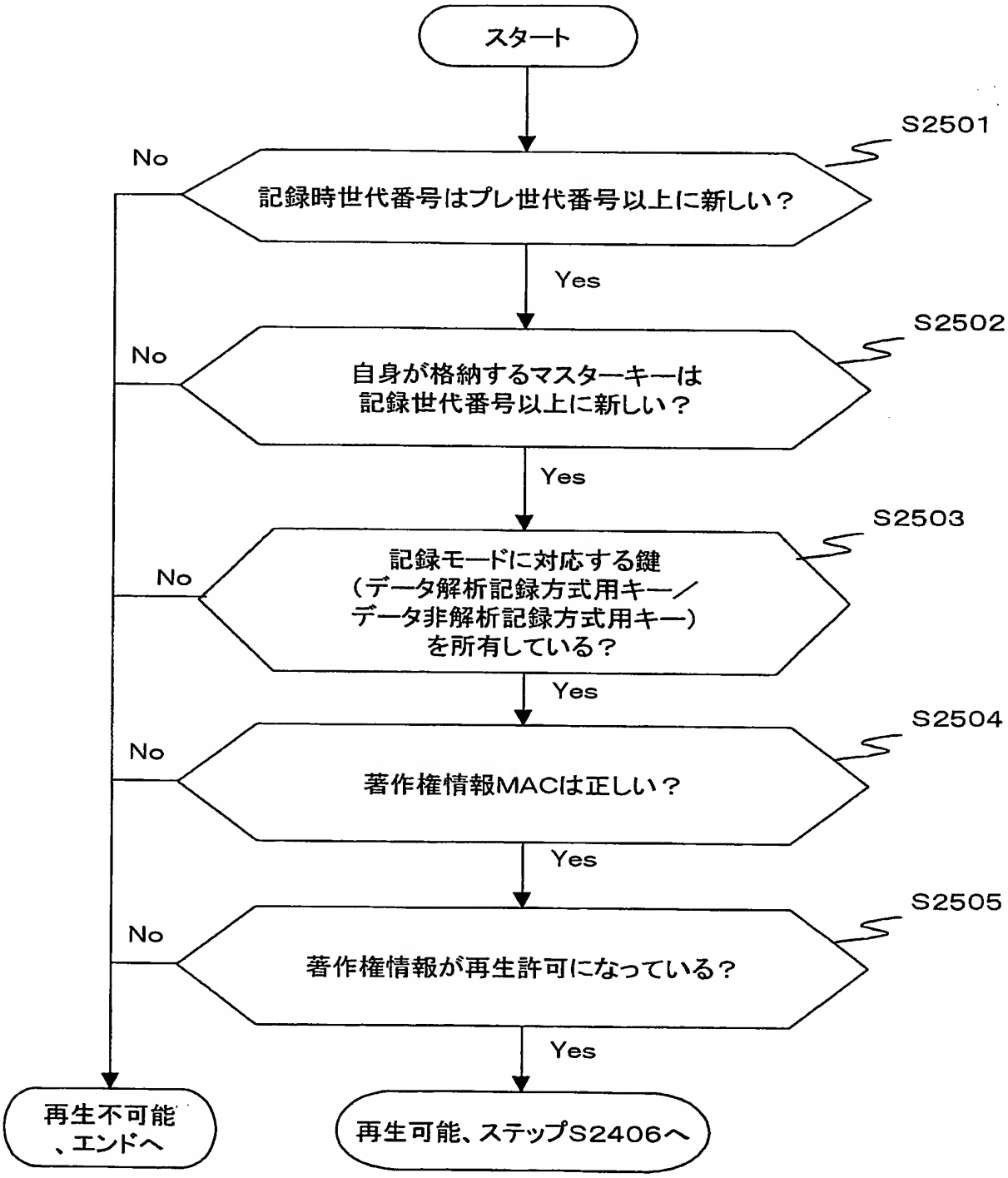

スタート
S2501
No
記録時世代番号はプレ世代番号以上に新しい？
Yes
S2502
No
自身が格納するマスターキーは
記録世代番号以上に新しい？
Yes
S2503
No
記録モードに対応する鍵
（データ解析記録方式用キー／
データ非解析記録方式用キー）
を所有している？
Yes
S2504
No
著作権情報MACは正しい？
Yes
S2505
No
著作権情報が再生許可になっている？
Yes
再生不可能
、エンドへ
再生可能、ステップS2406へ

Fig.33

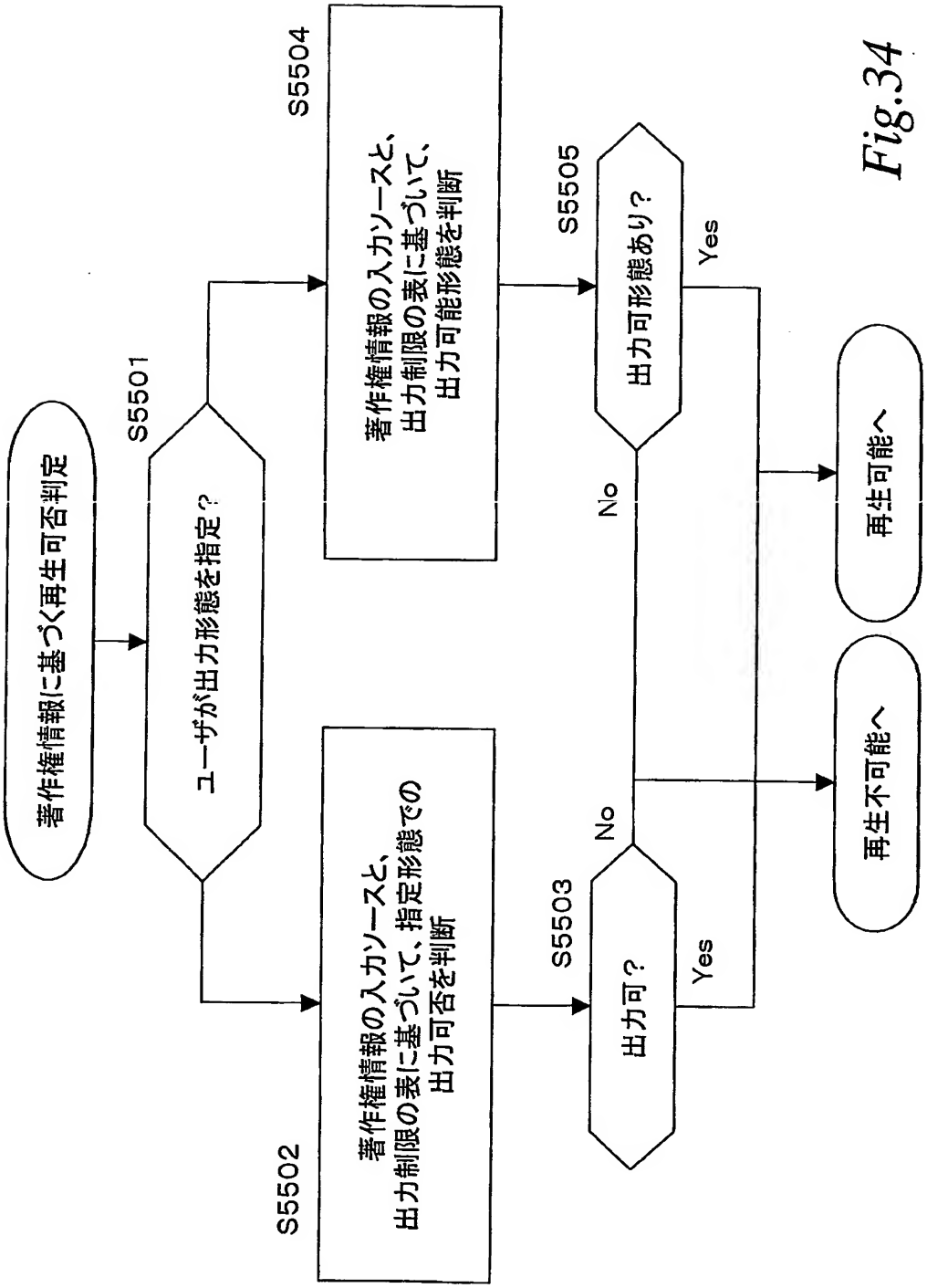

著作権情報に基づく再生可否判定
S5501
ユーザが出力形態を指定？
S5502
著作権情報の入力ソースと、
出力制限の表に基づいて、指定形態での
出力可否を判断
S5503
出力可？
No
Yes
S5504
著作権情報の入力ソースと、
出力制限の表に基づいて、
出力可能形態を判断
S5505
出力可形態あり？
No
Yes
再生不可能へ
再生可能へ

Fig.34

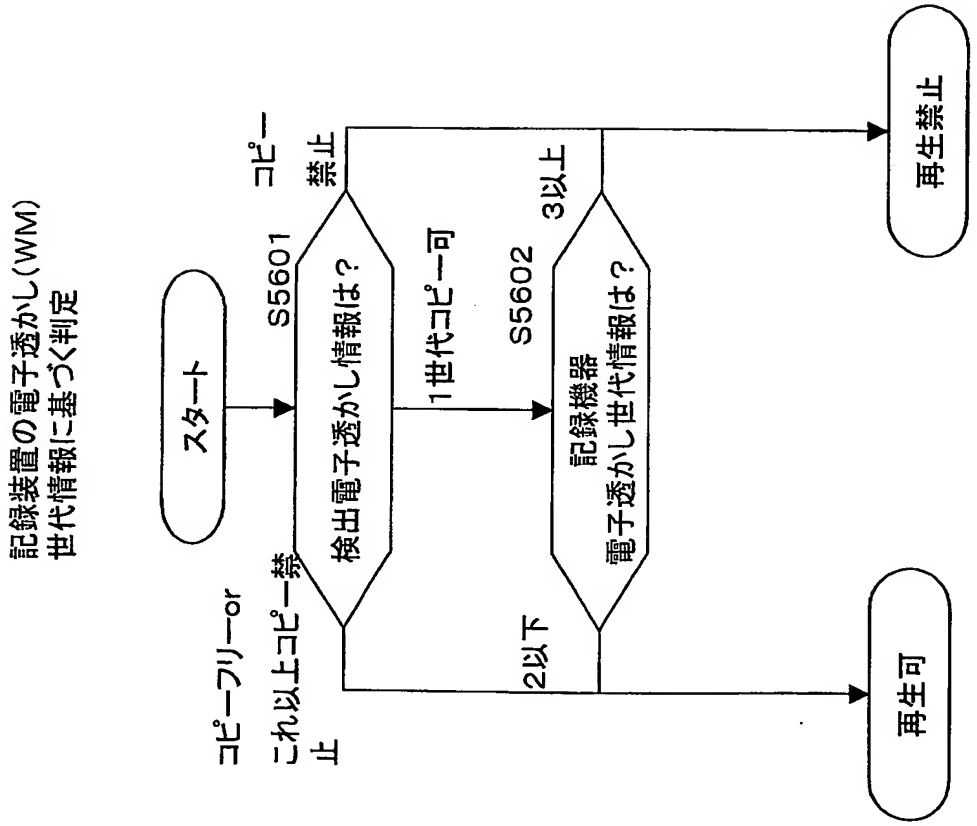

記録装置の電子透かし(WM)
世代情報に基づく判定
スタート
S5601
検出電子透かし情報は？
コピーフリーor
これ以上コピー禁止
コピー禁止
1世代コピー可
S5602
記録機器
電子透かし世代情報は？
3以上
2以下
再生禁止
再生可

Fig.35

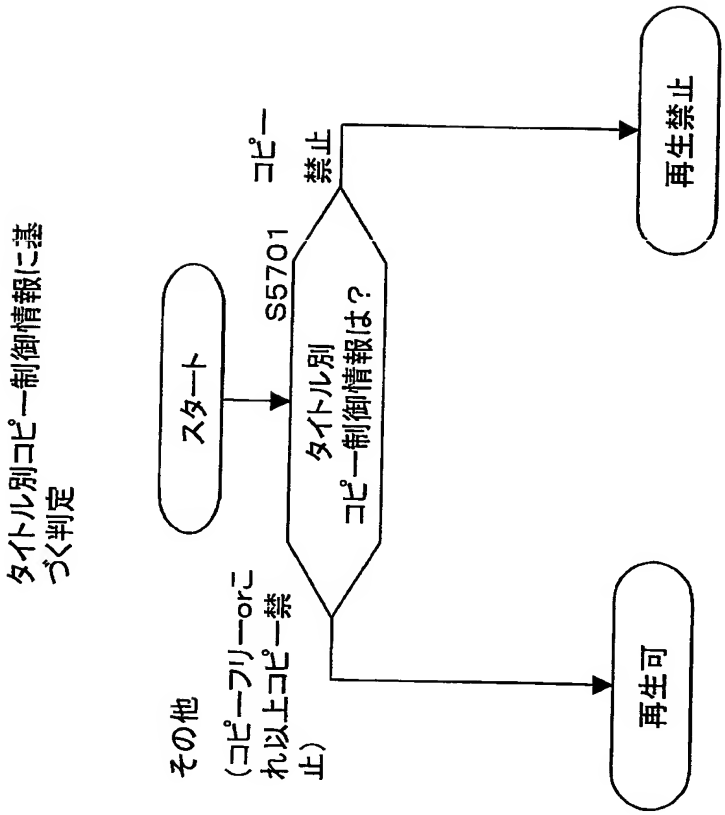

タイトル別コピー制御情報に基づく判定
スタート
S5701
タイトル別
コピー制御情報は？
コピー禁止
再生禁止
その他
(コピーフリーorこれ以上コピー禁止)
再生可

Fig.36

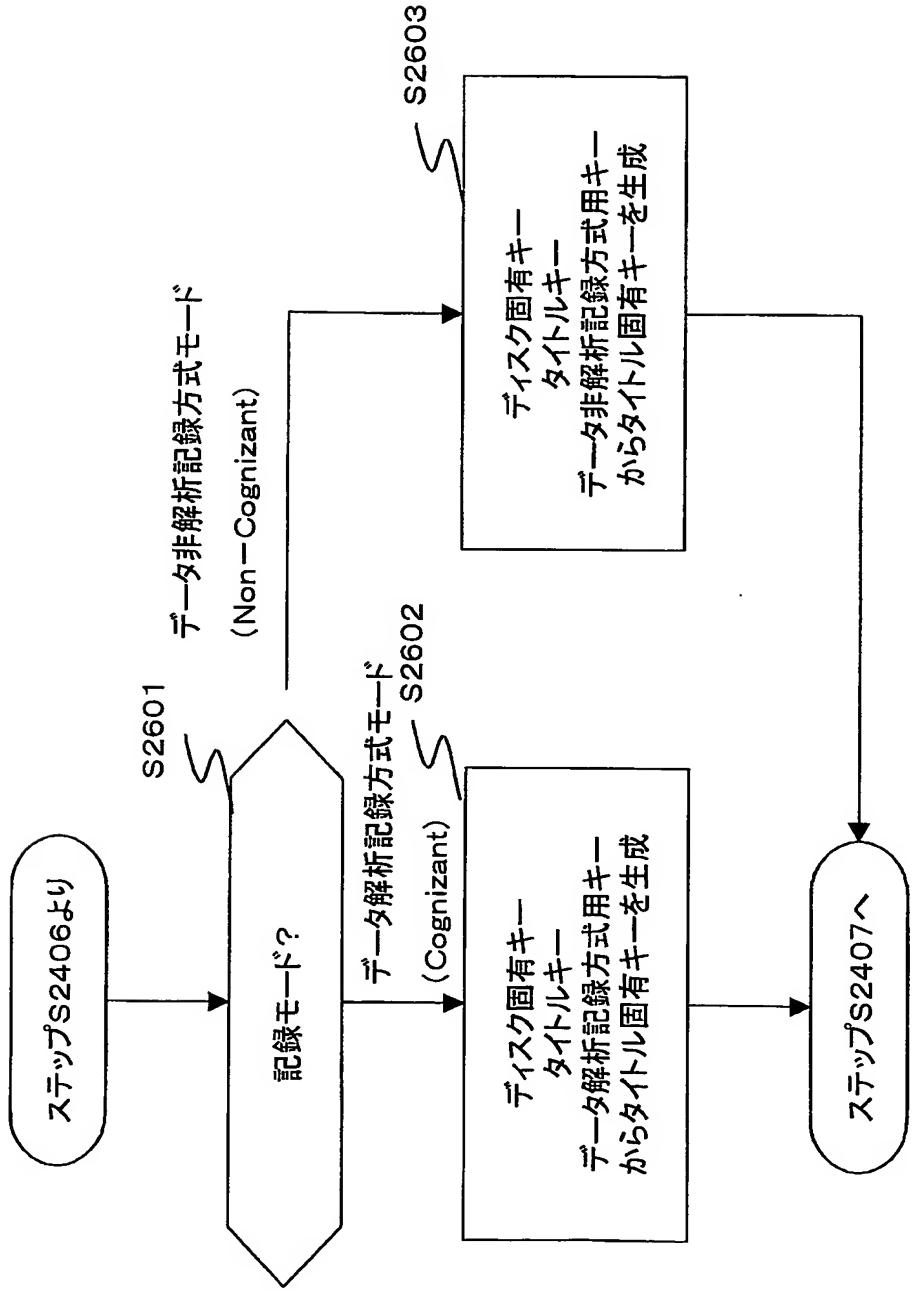

ステップS2406より
S2601
記録モード?
データ非解析記録方式モード
(Non−Cognizant)
S2603
ディスク固有キー
タイトルキー
データ非解析記録方式用キー
からタイトル固有キーを生成
データ解析記録方式モード
(Cognizant)
S2602
ディスク固有キー
タイトルキー
データ解析記録方式用キー
からタイトル固有キーを生成
ステップS2407へ

Fig.37

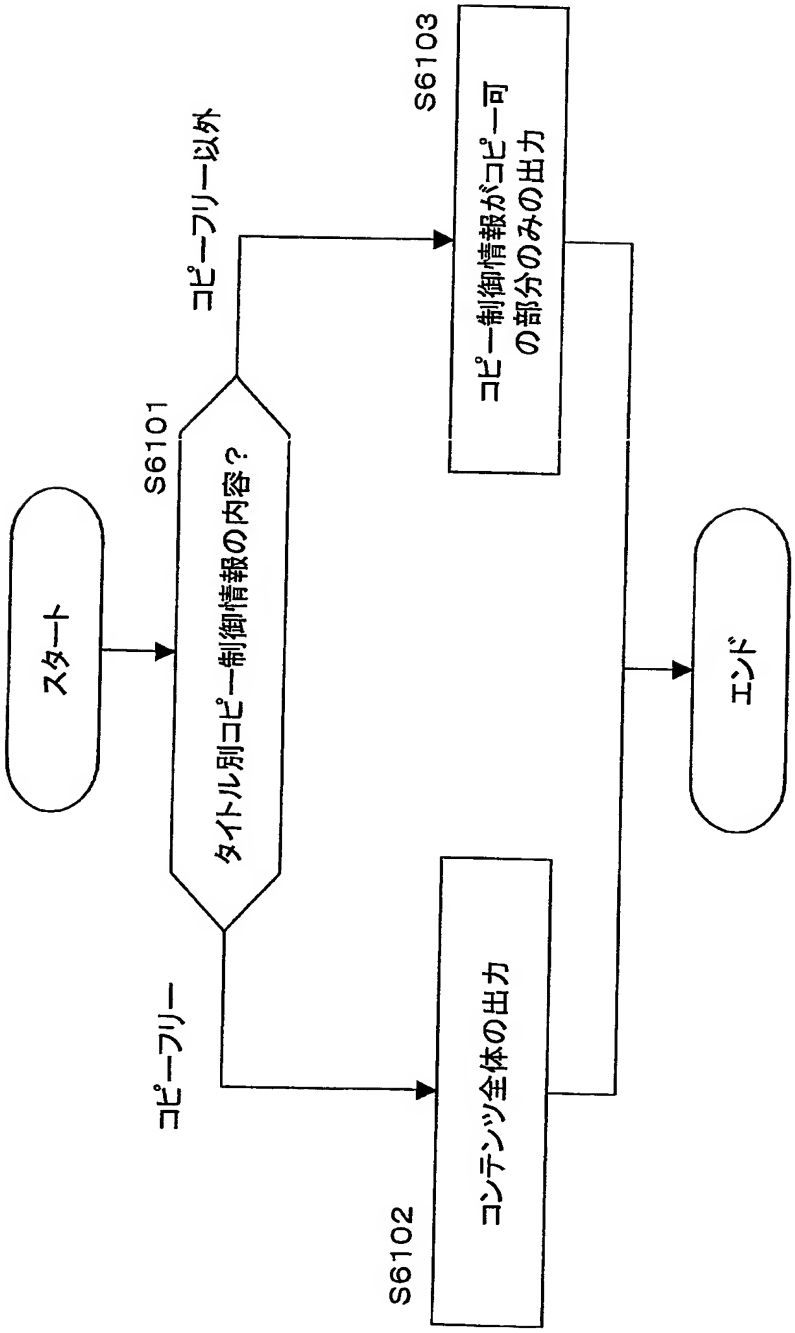
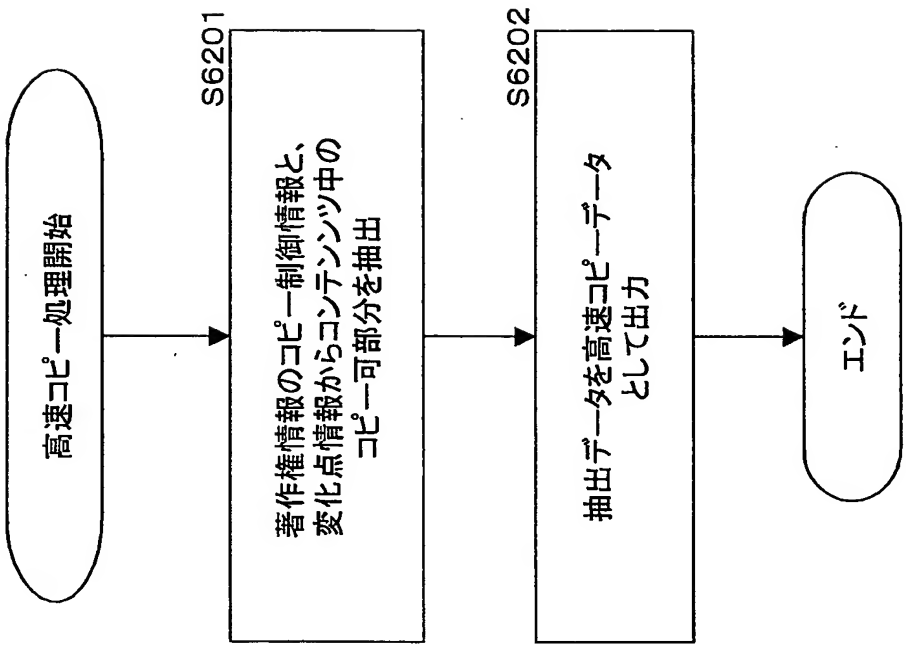

スタート
S6101
タイトル別コピー制御情報の内容？
コピーフリー以外
コピーフリー
S6103
コピー制御情報がコピー可の部分のみの出力
S6102
コンテンツ全体の出力
エンド

Fig.38

Fig.39


高速コピー処理開始
S6201
著作権情報のコピー制御情報と、
変化点情報からコンテンツ中の
コピー可部分を抽出
S6202
抽出データを高速コピーデータ
として出力
エンド

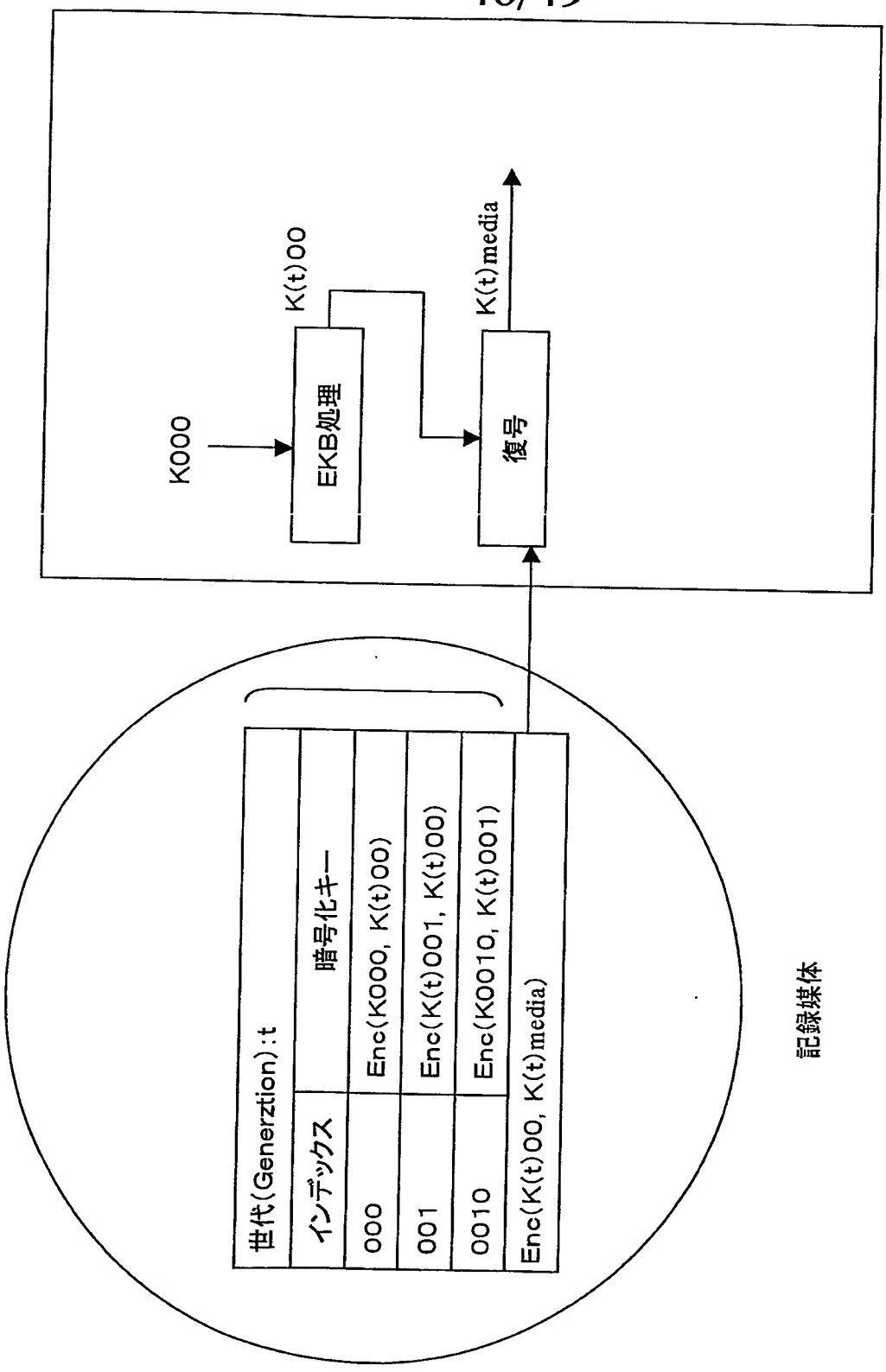

K000
EKB処理
K(t)00
復号
K(t)media
デバイス0
記録媒体
世代(Generztion):t
インデックス
暗号化キー
000
Enc(K000, K(t)00)
001
Enc(K(t)001, K(t)00)
0010
Enc(K0010, K(t)001)
Enc(K(t)00, K(t)media)

Fig.40

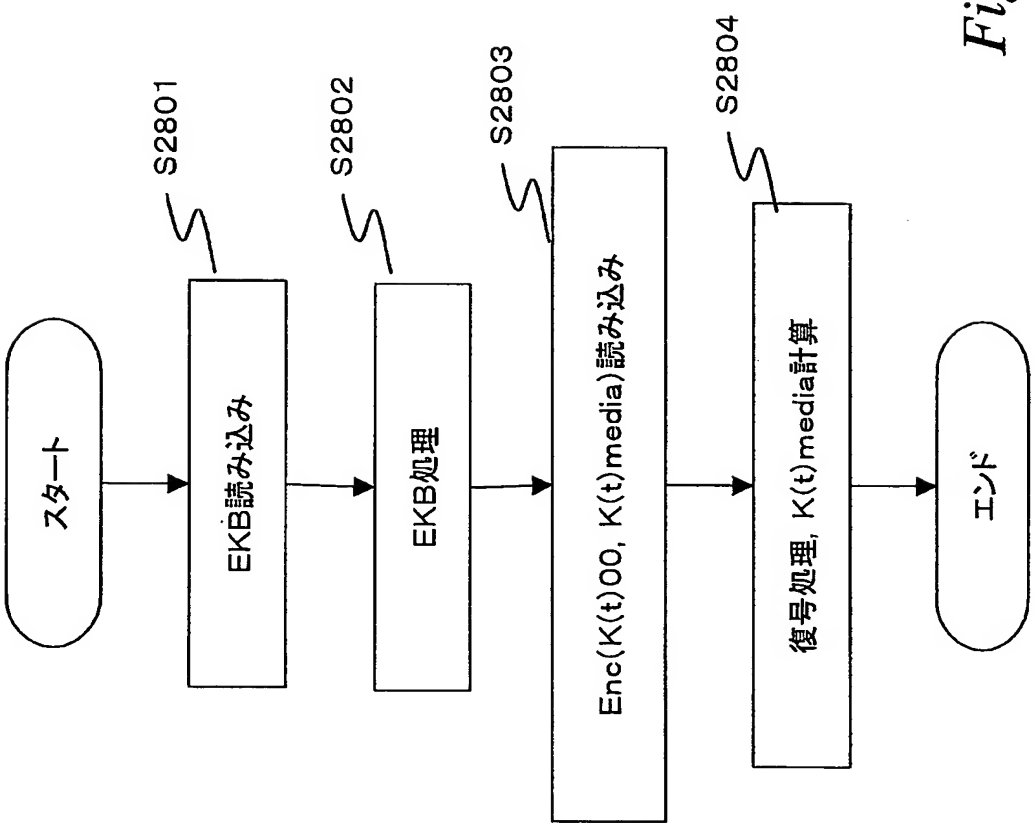
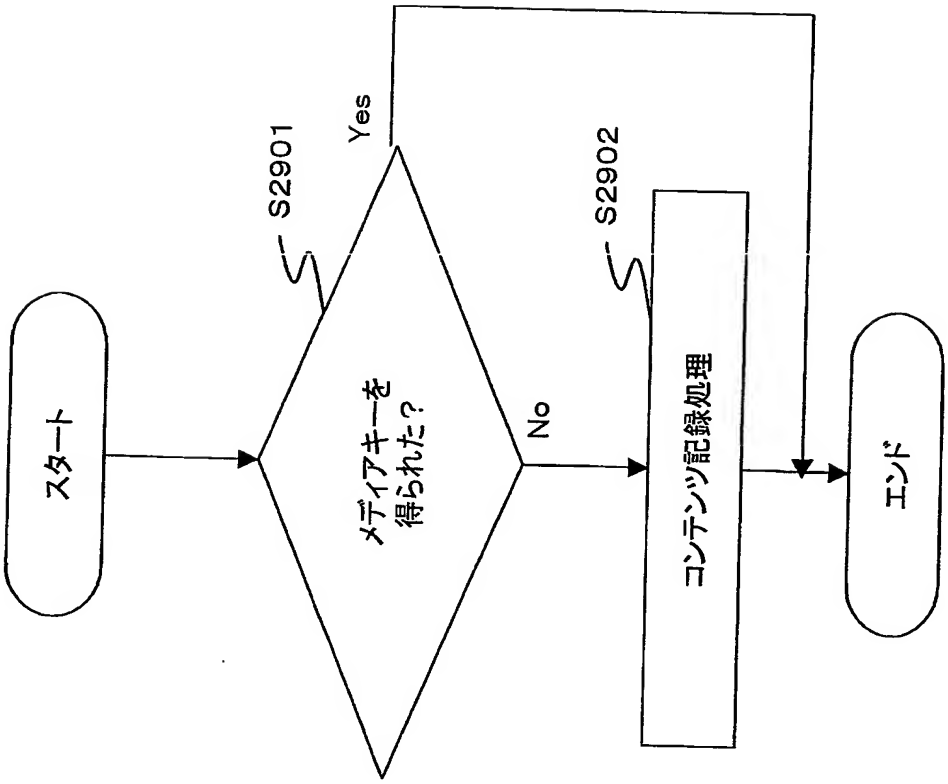

スタート
S2801
EKB読み込み
S2802
EKB処理
S2803
Enc(K(t)00, K(t)media)読み込み
S2804
復号処理, K(t)media計算
エンド

Fig.41

Fig.42



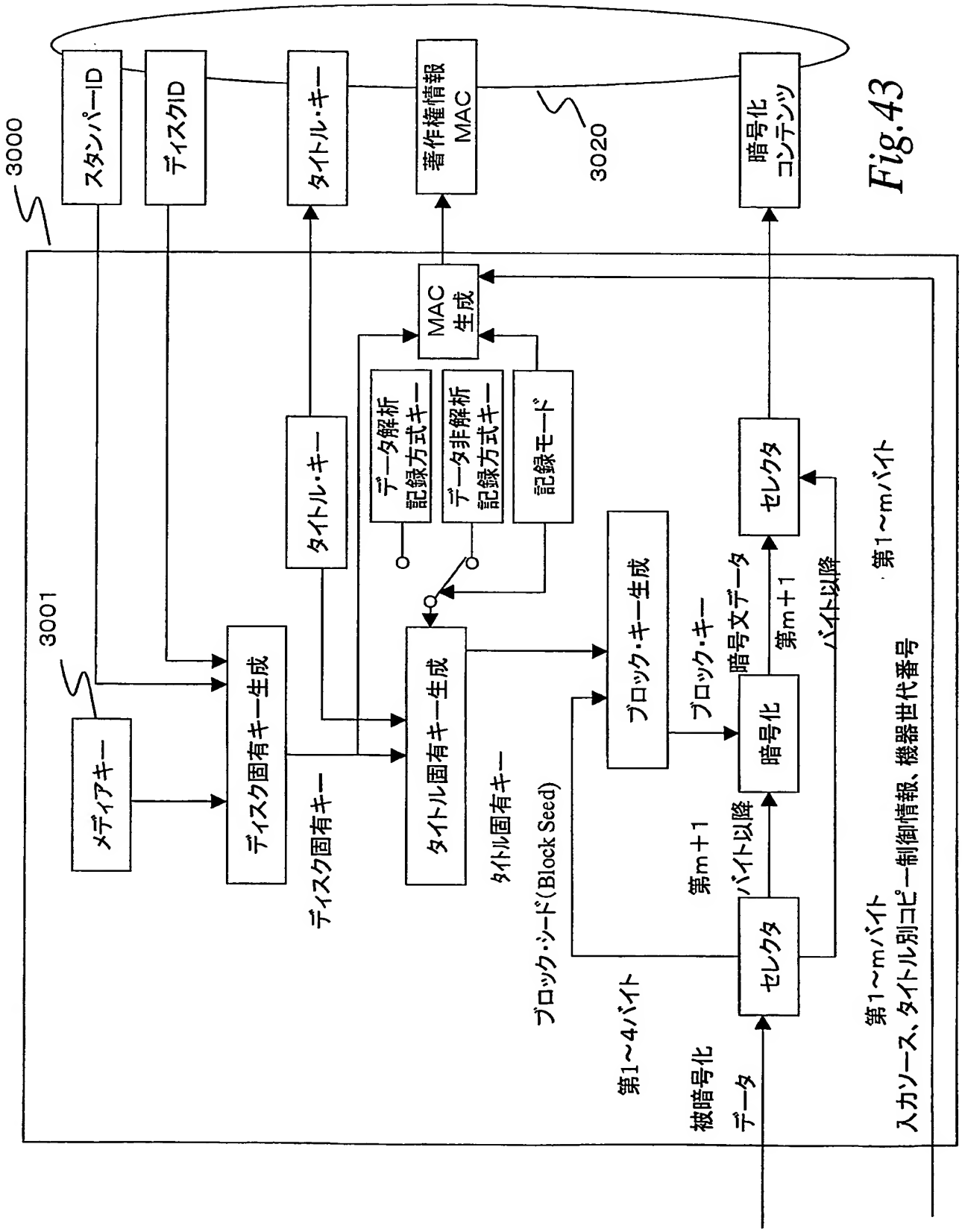

3000
スタンパーID
ディスクID
タイトル・キー
著作権情報
MAC
3020
暗号化
コンテンツ
MAC
生成
データ解析
記録方式キー
データ非解析
記録方式キー
記録モード
タイトル・キー
3001
メディアキー
ディスク固有キー生成
ディスク固有キー
タイトル固有キー生成
タイトル固有キー
ブロック・シード(Block Seed)
ブロック・キー生成
ブロック・キー
暗号文データ
暗号化
セレクタ
第m＋1
バイト以降
セレクタ
第m＋1
バイト以降
第1～4バイト
被暗号化
データ
第1～mバイト
入力ソース、タイトル別コピー制御情報、機器世代番号
第1～mバイト

Fig.43

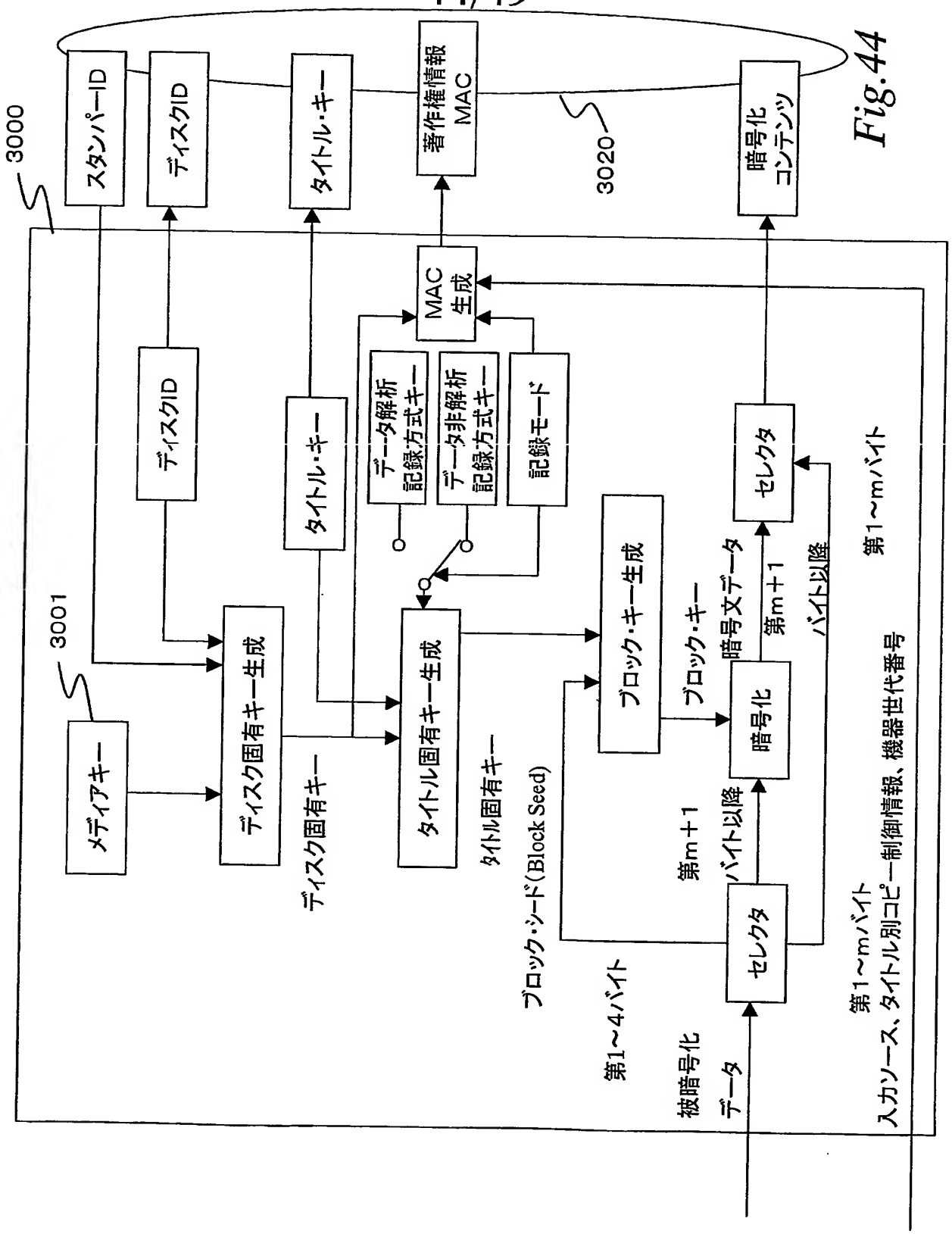

3000
スタンパーID
ディスクID
タイトル・キー
著作権情報 MAC
3020
暗号化コンテンツ
MAC生成
ディスクID
タイトル・キー
データ解析記録方式キー
データ非解析記録方式キー
記録モード
3001
メディアキー
ディスク固有キー生成
ディスク固有キー
タイトル固有キー生成
タイトル固有キー
ブロック・キー生成
ブロック・シード(Block Seed)
第1～4バイト
ブロック・キー
暗号文データ
第m＋1
バイト以降
暗号化
セレクタ
バイト以降
セレクタ
第1～mバイト
被暗号化データ
第1～mバイト
入力ソース、タイトル別コピー制御情報、機器世代番号

Fig.44

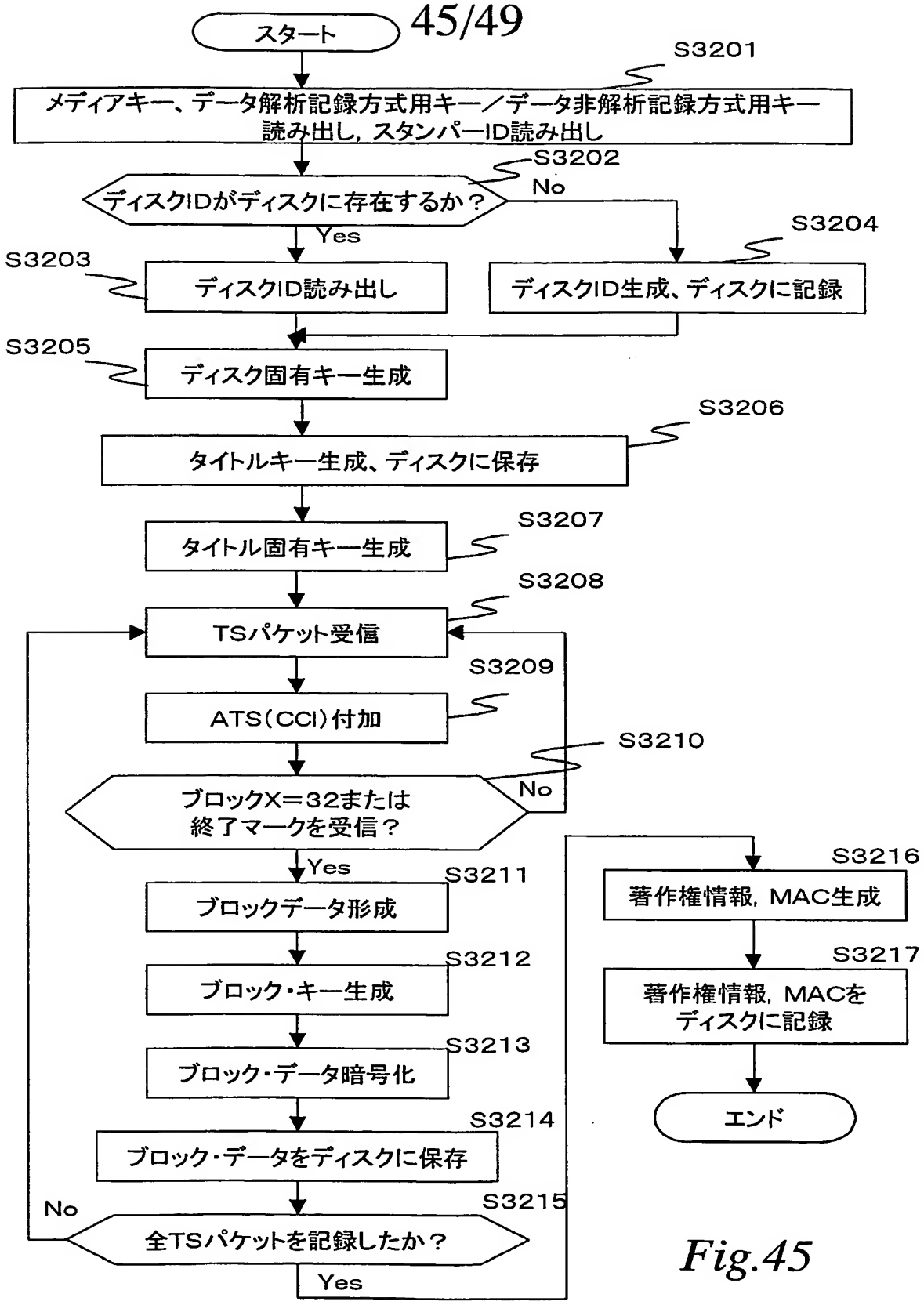

スタート
S3201
メディアキー、データ解析記録方式用キー／データ非解析記録方式用キー読み出し，スタンパーID読み出し
S3202
ディスクIDがディスクに存在するか？
No
Yes
S3203
ディスクID読み出し
S3204
ディスクID生成、ディスクに記録
S3205
ディスク固有キー生成
S3206
タイトルキー生成、ディスクに保存
S3207
タイトル固有キー生成
S3208
TSパケット受信
S3209
ATS(CCI)付加
S3210
ブロックX=32または終了マークを受信？
No
Yes
S3211
ブロックデータ形成
S3212
ブロック・キー生成
S3213
ブロック・データ暗号化
S3214
ブロック・データをディスクに保存
S3215
No
全TSパケットを記録したか？
Yes
S3216
著作権情報，MAC生成
S3217
著作権情報，MACをディスクに記録
エンド

Fig.45

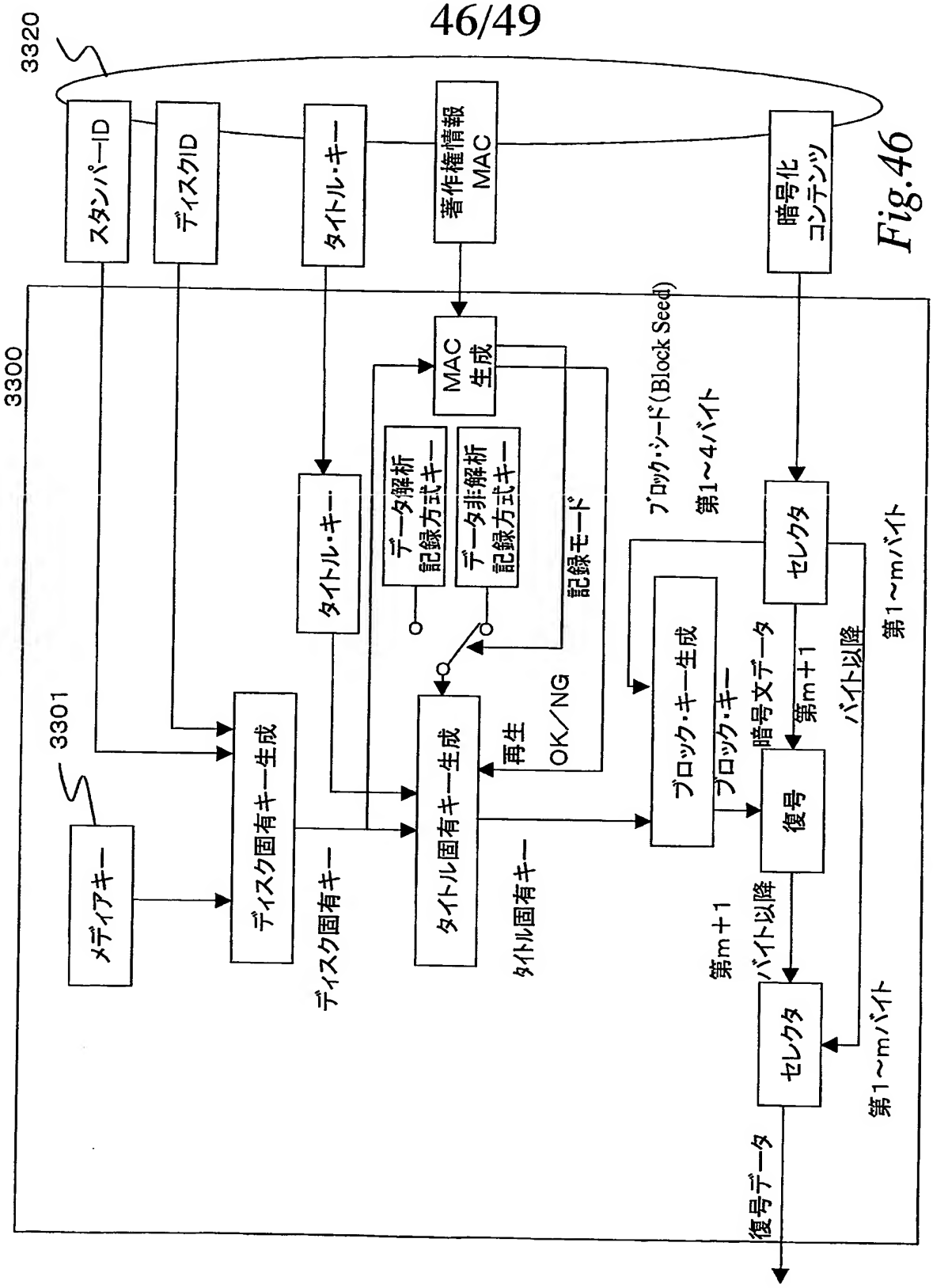

3320
スタンパーID
ディスクID
タイトル・キー
著作権情報 MAC
暗号化コンテンツ
3300
MAC 生成
データ解析記録方式キー
データ非解析記録方式キー
タイトル・キー
記録モード
ブロック・シード(Block Seed)
第1～4バイト
セレクタ
第1～mバイト
3301
メディアキー
ディスク固有キー生成
ディスク固有キー
タイトル固有キー生成
再生
OK／NG
タイトル固有キー
ブロック・キー生成
ブロック・キー
暗号文データ
第m＋1
バイト以降
復号
第m＋1
バイト以降
セレクタ
第1～mバイト
復号データ

Fig.46

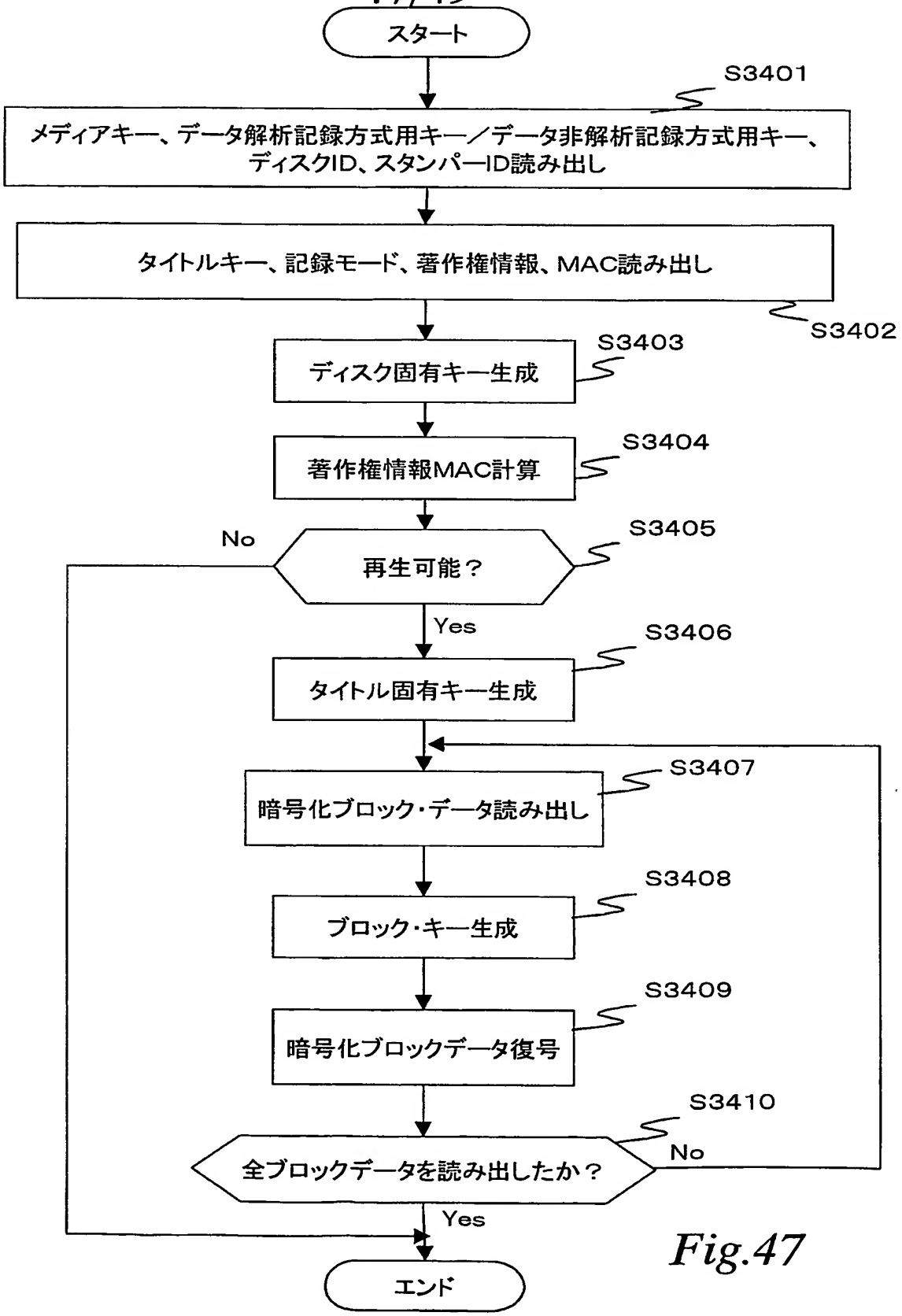

スタート
S3401
メディアキー、データ解析記録方式用キー／データ非解析記録方式用キー、
ディスクID、スタンパーID読み出し
タイトルキー、記録モード、著作権情報、MAC読み出し
S3402
S3403
ディスク固有キー生成
S3404
著作権情報MAC計算
S3405
No
再生可能？
Yes
S3406
タイトル固有キー生成
S3407
暗号化ブロック・データ読み出し
S3408
ブロック・キー生成
S3409
暗号化ブロックデータ復号
S3410
全ブロックデータを読み出したか？
No
Yes
エンド

Fig.47

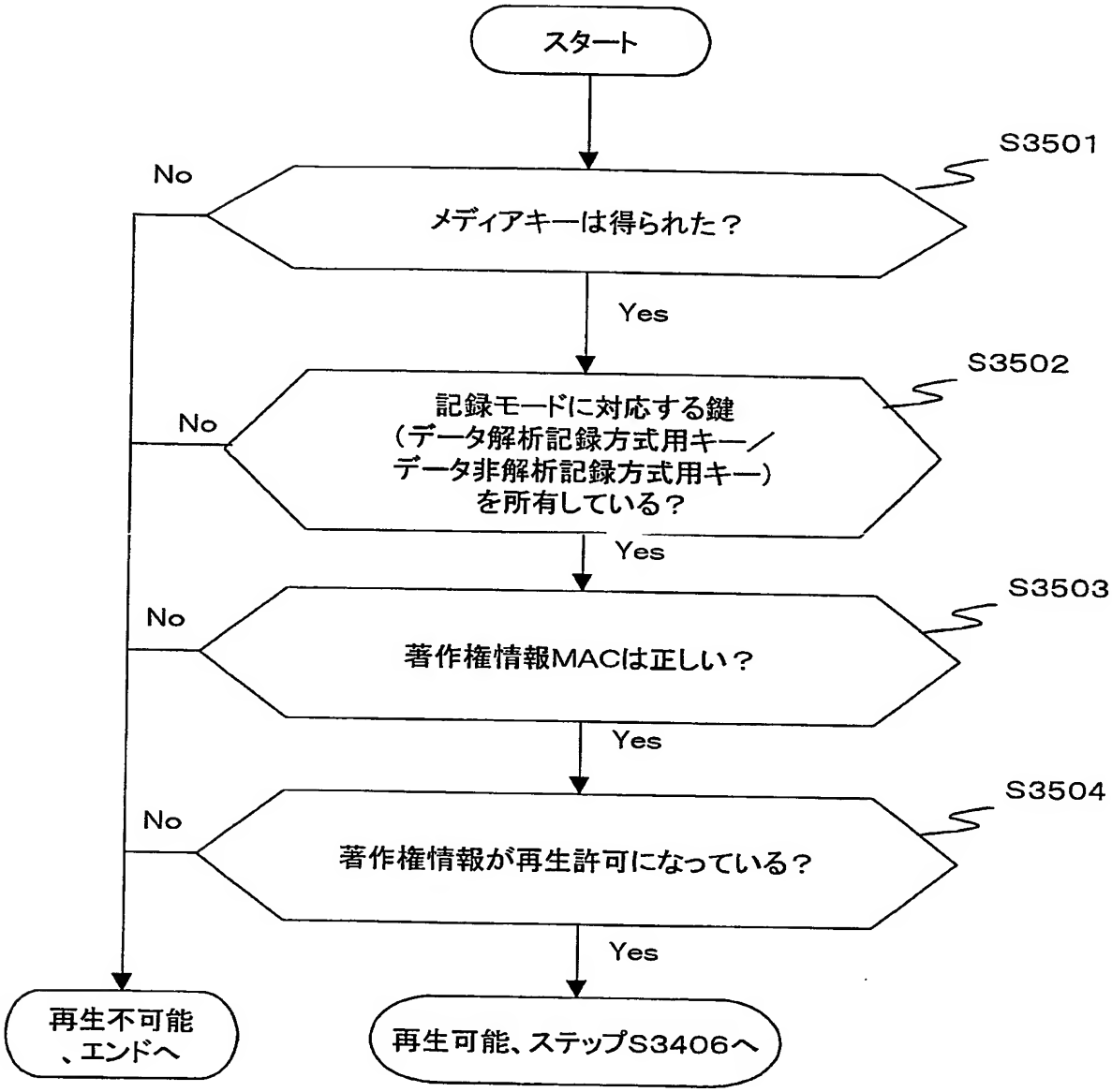

スタート
S3501
No
メディアキーは得られた？
Yes
S3502
No
記録モードに対応する鍵
（データ解析記録方式用キー／
データ非解析記録方式用キー）
を所有している？
Yes
S3503
No
著作権情報MACは正しい？
Yes
S3504
No
著作権情報が再生許可になっている？
Yes
再生不可能
、エンドへ
再生可能、ステップS3406へ

Fig.48

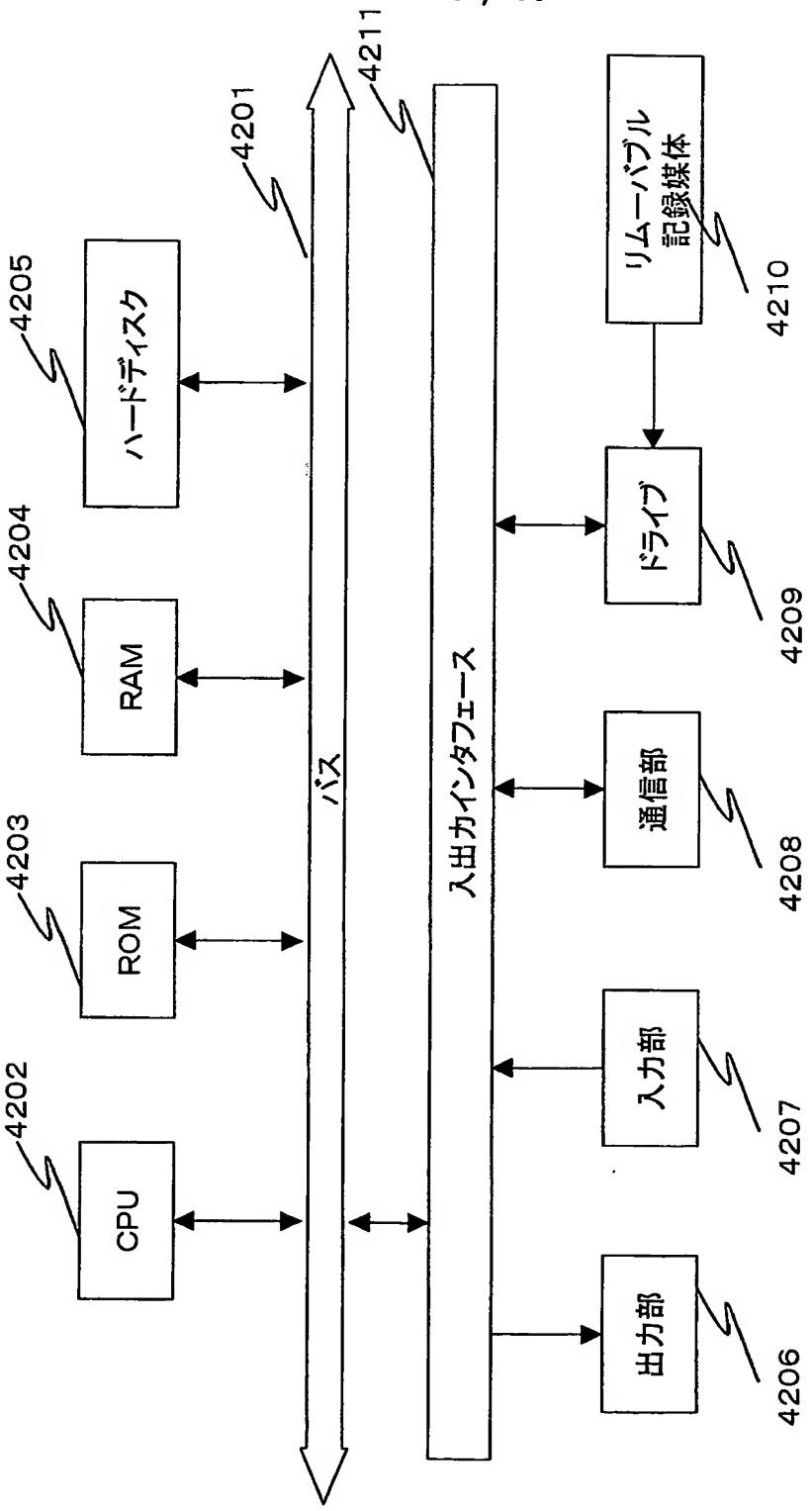

4211
4201
4205
ハードディスク
4204
RAM
4203
ROM
4202
CPU
バス
入出力インタフェース
リムーバブル記録媒体
4210
ドライブ
4209
通信部
4208
入力部
4207
出力部
4206

Fig.49

INTERNATIONAL SEARCH REPORT

International application No.
PCT/JP02/07477

A. CLASSIFICATION OF SUBJECT MATTER
Int.Cl[7] G11B20/10, H04L9/08, H04N5/91

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)
Int.Cl[7] G11B20/10, H04L9/08, H04N5/91

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Jitsuyo Shinan Koho	1922-1996	Toroku Jitsuyo Shinan Koho	1994-2002
Kokai Jitsuyo Shinan Koho	1971-2002	Jitsuyo Shinan Toroku Koho	1996-2002

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
Y	WO 00/62476 A1 (Sony Corp.), 19 October, 2000 (19.10.00), Full text; Figs. 1 to 9 (Family: none)	1-30
Y	JP 5-327748 A (Fujitsu Ltd.), 10 December, 1993 (10.12.93), Full text; Figs. 1 to 19 (Family: none)	1-30
Y	JP 2001-36517 A (Lucent Technologies Inc.), 09 February, 2001 (09.02.01), Full text; Figs. 1 to 9 (Family: none)	1-30

[X] Further documents are listed in the continuation of Box C. [ ] See patent family annex.

* Special categories of cited documents:
"A" document defining the general state of the art which is not considered to be of particular relevance
"E" earlier document but published on or after the international filing date
"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)
"O" document referring to an oral disclosure, use, exhibition or other means
"P" document published prior to the international filing date but later than the priority date claimed
"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention
"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone
"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art
"&" document member of the same patent family

Date of the actual completion of the international search 24 September, 2002 (24.09.02)	Date of mailing of the international search report 08 October, 2002 (08.10.02)
Name and mailing address of the ISA/ Japanese Patent Office Facsimile No.	Authorized officer Telephone No.

Form PCT/ISA/210 (second sheet) (July 1998)

INTERNATIONAL SEARCH REPORT

International application No.
PCT/JP02/07477

C (Continuation). DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	JP 11-308564 A (Olympus Optical Co., Ltd.), 05 November, 1999 (05.11.99), Full text; Figs. 1 to 17 (Family: none)	2,6-7,9, 13-14,16, 20-21,27-28
A	JP 2001-125833 A (Sony Corp.), 11 May, 2001 (11.05.01), Full text; Figs. 1 to 31 (Family: none)	2,6-7,9, 13-14,16, 20-21,27-28

国際調査報告

国際出願番号　PCT／JP02／07477

A.　発明の属する分野の分類（国際特許分類（IPC））

Int. Cl⁷　G11B 20／10　H04L 9／08　H04N 5／91

B.　調査を行った分野

調査を行った最小限資料（国際特許分類（IPC））

Int. Cl⁷　G11B 20／10　H04L 9／08　H04N 5／91

最小限資料以外の資料で調査を行った分野に含まれるもの

日本国実用新案公報　1922－1996年
日本国公開実用新案公報　1971－2002年
日本国登録実用新案公報　1994－2002年
日本国実用新案登録公報　1996－2002年

国際調査で使用した電子データベース（データベースの名称、調査に使用した用語）

C.　関連すると認められる文献

引用文献のカテゴリー＊	引用文献名　及び一部の箇所が関連するときは、その関連する箇所の表示	関連する請求の範囲の番号
Y	WO 00/62476 A1　（ソニー株式会社） 2000. 10. 19 ，全文，　第1－9図　（ファミリーなし）	1-30
Y	JP 5-327748 A（富士通株式会社） 1993. 12. 10 ，全文，　第1－19図　（ファミリーなし）	1-30

☒ C欄の続きにも文献が列挙されている。　☐ パテントファミリーに関する別紙を参照。

＊　引用文献のカテゴリー
「A」特に関連のある文献ではなく、一般的技術水準を示すもの
「E」国際出願日前の出願または特許であるが、国際出願日以後に公表されたもの
「L」優先権主張に疑義を提起する文献又は他の文献の発行日若しくは他の特別な理由を確立するために引用する文献（理由を付す）
「O」口頭による開示、使用、展示等に言及する文献
「P」国際出願日前で、かつ優先権の主張の基礎となる出願の日の後に公表された文献
「T」国際出願日又は優先日後に公表された文献であって出願と矛盾するものではなく、発明の原理又は理論の理解のために引用するもの
「X」特に関連のある文献であって、当該文献のみで発明の新規性又は進歩性がないと考えられるもの
「Y」特に関連のある文献であって、当該文献と他の1以上の文献との、当業者にとって自明である組合せによって進歩性がないと考えられるもの
「&」同一パテントファミリー文献

国際調査を完了した日	国際調査報告の発送日
24. 09. 02	08.10.02

国際調査機関の名称及びあて先	特許庁審査官（権限のある職員）		
日本国特許庁（ISA／JP） 郵便番号100－8915 東京都千代田区霞が関三丁目4番3号	宮下　誠	5Q	2946
	電話番号　03－3581－1101　内線　3590		

様式PCT／ISA／210（第2ページ）（1998年7月）

国際調査報告	国際出願番号　ＰＣＴ／ＪＰ０２／０７４７７

C（続き）．　関連すると認められる文献

引用文献のカテゴリー＊	引用文献名　及び一部の箇所が関連するときは、その関連する箇所の表示	関連する請求の範囲の番号
Y	ＪＰ　2001-36517　Ａ（ルーセント　テクノロジーズ　インコーポレイテッド） 2001. 02. 09　，全文，　第1－9図　（ファミリーなし）	1-30
A	ＪＰ　11-308564　Ａ（オリンパス光学工業株式会社） 1999. 11. 05　，全文，　第1－17図　（ファミリーなし）	2、6-7、9、13-14、16、20-21、27-28
A	ＪＰ　2001-125833　Ａ（ソニー株式会社） 2001. 05. 11　，全文，　第1－31図　（ファミリーなし）	2、6-7、9、13-14、16、20-21、27-28